KENYA REVENUE AUTHORITY

MULTI-VENDOR-USER OWNED ESEALS FRAMEWORK

QUALIFICATION OF VENDORS FOR

SUPPLY, OPERATION, MAINTENANCE AND MANAGED SERVICES OF

ELECTRONIC SEALS

TABLE OF CONTENT

TERMS OF REFFEENCE

KRA	**Kenya Revenue Authority.**
RAs	**REVENUE Authority’s.**
EAC	**EAST African Community.**
EACCMA	**East African Community Customs Managemnt Act**
EACCMAR	**EAST African Community Customs Managemnt Act Regulations.**
RECTS	**Regional Electronic Cargo Tracking System.**
CFA	**Cearing & Forwading Agents.**
SCT	**Single Customs Territory.**
KPI	**Key Perfomance Indicators.**
IT	**Information Technology.**
IoT	**Internet Of Things.**
DRC	**Democratic Republic Of Congo.**
KPA	**Kenya Port Authority.**
CFS	**Container Freight Station.**
ICD	**Inland Conatiner Deport.**
SOP	**Standard Operations Procedures.**
MOU	**Memorandum Of Understanding.**
RFID	**Radio Frequency Identification.**
CMU	**Cargo Monitoring Unit.**
RRU	**Response Unit.**
GPRS	**General Packet Radio Service.**
GPS	**Global Positioning System.**
GSM	**Global System For Mobile Communications.**
OCR	**Optical Character Recognition.**
OR	**Object Reader.**
CBWHSE	**Customs Bonded Werehouse.**
CAK	**Communications Authority Of Kenya.**
QA	**Quality Assuarance.**
MO	**Maintenance Office.**
TRA	**Tanzania Revenue Authority.**
URA	**Uganda Revenue Authority.**
RRA	**Rwanda Revenue Authority.**
OBR	**Burundi Revenue.**
DGDA	**Direction Générale Des Douanes Et Accises.**
SSRA	**South Sudan Revenue Authority.**
EPZ	**Processing Zones.**
VAT	**Value Added Tax.**
TCP	**Tran.smission Control Protocol.**
HTTP	**Hypertext Transfer Protocol.**
TLS	**Transport Layer Security.**
DNS	**Domain Name System.**
FQDN	**Fully Qualified Domain Name.**
HDOP	**Horizontal Dilution Of Precision.**
LAC	**Location Area Code.**
MCC	**Mobile Country Code.**

SECTION I:
SCHEDULE OF REQUIREMENTS

1. SCHEDULE OF SUPPLIES AND RELATED SERVICES

Kenya Revenue Authority (KRA) intends to enter into **framework contracts with Qualified Vendors** for the **Supply, Operation, Maintenance, and Managed Services of Electronic eSeals** and associated equipment under the **Regional Electronic Cargo Tracking System (EAC RECTS)**.

1.1 Contractual Model

The engagement shall operate under a **self-financing model**, whereby:

- The vendor will be approved by KRA as per the conditions specified in this document
- The service provider shall have the uniquely identifiable seals/e-fuel seals that shall be registered in the EAC RECTS platform,
- The vendor will not be expected to maintain a parallel dashboard but will be given access to EAC RECTS to monitor and manage his e-seals or integrate to the EAC RECTS through an API protocol,
- The vendor will be jointly and severally liable for goods lost in transit if the seals do not report the non-compliant activity or if the vendor is found to have colluded with the other parties in line with Customs Laws and procedures.
- KRA reserves the right to intervene to ensure fairness, transparency, service continuity, and compliance.
- Approved Vendors shall ensure continuous availability of well-maintained, standardized and EAC RECTS compliant electronic seals.

1.2 Scope of Supplies and Services

Seals Service Provider Vendor shall provide the following items and services:

S/N	Description	Unit

1	Electronic Seals Supply	
2	Electronic Seals Logistics Services	
3	Electronic Seal Maintenance, Repair, Charging, Calibration and Quality Assurance (Pre-Departure Checks) Services	

SECTION II:

TECHNICAL REQUIREMENTS FOR ELECTRONIC SEALS

Scope of Works and Operational Requirements

1. INTRODUCTION

This document sets out the **technical, operational, and compliance requirements** for qualification of Vendors for supply of electronic seals and related services for the EAC RECTS platform.

2. BACKGROUND

The **Regional Electronic Cargo Tracking System (RECTS)** enables real-time monitoring of cargo in transit and other Customs-controlled goods. Introduced by KRA in 2017, the system was adopted in 2022 by the **East African Community (EAC) Secretariat** as the **EAC RECTS**.
The system enhances customs control, trade facilitation, and revenue protection through digital monitoring, geo-fencing, and automated alerts.

3. OBJECTIVES OF ELECTRONIC CARGO MONITORING

Implementation of Electronic cargo monitoring using e-seals aims to:

a. Provide real-time visibility of cargo in transit
b. Increase revenue collection and compliance
c. Reduce transit times and operational costs
d. Enhance transparency and integrity
e. Enable rapid incident response
f. Generate comprehensive surveillance and investigation reports
g. Support Bond activation and deactivation
h. Improve truck turnaround time and ease of doing business

4. PURPOSE OF THE DOCUMENT

The purpose of this document is to **qualify Vendors** capable of supplying **fully compliant electronic eseals and related services** for integration into the **EAC RECTS platform**, under a self-financing framework arrangement.

5. SCOPE OF ENGAGEMENT

5.1 Vendor approval and operationalization

All devices submitted must be 100% compliant with EAC RECTS technical standards.

5.1.1 Devices must be fully integrated with the EAC RECTS Platform

5.1.2 Vender approval shall only be granted in two stages

a. Stage 1 Approval: Vendor and Electronic seal device approval

b. Stage 2 Approval: Successful integration with ECTS RECTS Platform

5.1.3 Vendor shall on be allowed to operationalize the e-seals only after stage 2 approval.

5.2 Operational Framework

Qualified Vendors shall be approved to operate for a period of **two (2)-years**, **subject to monthly performance and compliance reviews being met. KRA reserves the right to suspend, reinstate or cancel the approval.**

6. OPERATIONAL AND TECHNICAL REQUIREMENTS

6.1 System Performance

Electronic seals deployed under EAC RECTS shall meet the following minimum performance thresholds:

a. **Real-time event alerting:** Transmission of critical alerts, or incidences within **two (2) seconds** of occurrence.

b. **Location reporting:** Automated GPS position updates at configurable time interval (Over the Air or physically) as per KRA request default setting should be **five-minute intervals** throughout the transit period.

c. **Data continuity:** Uninterrupted reporting capability for a minimum duration of **sixty (60) consecutive days** on a single charge

d. **Positioning and communication:** Use of Dual Global Navigation Satellite System (GNSS) **for positioning** and **2G/3G/4G/5G or equivalent cellular technology** for data transmission to the EAC RECTS platform.

6.2 Business Model

Vendor owned and maintained eseals

Each Vendor shall submit a Self-Financing Business Plan demonstrating commercial viability and operational sustainability, including:

a. Audited financial statements for the last 3 years.

b. Vendor must provide:

- Device lifecycle management (repair, replacement, refurbishment).
- Regional workshops and repair hubs within EAC.
- Guaranteed turnaround time for seals.

7. OPERATIONAL COVERAGE REQUIREMENTS

7.1 Scope of Works

7.1.1 A fully functional EAC RECTS shall track all goods under customs control. Currently:

a. Approximately 60,000 trucks and tankers are licensed as means of conveyance.

b. About 80% of these road tankers are with four to six compartments.

c. Each truck or tanker shall be fitted with electronic seals, with all seal data captured by the EAC RECTS platform.

The main designated routes in the EAC RECTS Central platform include the following.

The principal road route runs from the coast to the Great Lakes region:

- **Mombasa → Nairobi → Nakuru → Eldoret → Bungoma → Malaba → Bugiri → Jinja → Kampala → Masaka → Katuna/Gatuna → Kigali → Nemba/Gasenyi → Ngozi → Kayanza → Bugarama → Bujumbura**.
- **Mombasa → Nairobi → Nakuru → Eldoret → Kitale → Lokichar → Lodwar → Kakuma → Lokichogio →**
- **Nadapal.**

- **Mombasa → Lamu → Garisa → Modegashe → Garbatula → Isiolo → Marsabit → Moyale**.

- **Total Length:** Approximately 2,080 km for the main route.
- **Alternative Route:** Mombasa → Kisumu → Busia → Kampala

Key Connector Roads

- **Kenya/Tanzania Connector**: Voi–Taveta/Holili–Moshi–Arusha (240 km).
- **Rwanda/DRC Connector**: Kigali to Goma/Bukavu.
- **Uganda/South Sudan**: Kampala-Nimule-Elegu (busiest border in South Sudan).

Additional routes may be designated by KRA as operational circumstances require

7.3 Operational Requirements

7.4.1 **Deployment and coverage:** Vendors shall deploy tagging and un-tagging officers at arming and disarming stations with **minimum 97% coverage**, including KPA port gates, CFS and ICD gates, Customs Bonded Warehouses, land border stations, and other customs-controlled areas. **KPA, CFS, and ICD gates are mandatory.**

7.4.2 **Staffing:** Continuous and adequate staffing shall be maintained at all arming and disarming locations.

7.4.3 **Device readiness:** Vendors shall ensure sufficient availability of devices ready for immediate deployment.

7.4.4 **Regulatory compliance:** Non-compliance shall constitute interference with goods under customs control, contrary to **Section 16(2)(b) read with Section 16(4) and Section 195 of the EAC-CMA, 2004**.

7.4.5 **Operating hours:** Vendor operations shall align with Customs operating hours. Failure to do so shall attract statutory sanctions and liability for losses arising from delayed service.

7.4.6 **Minimum stock:** Vendors shall maintain a minimum stock of **1,000 seals** at tender stage and throughout implementation. Stock depletion may result in suspension or contract termination at the discretion of the Commissioner of Customs and Excise.

7.4.7 **Seal functionality:** Vendors shall verify seal performance prior to tagging. Any malfunction during transit shall be rectified by **replacement within two (2) hours** of notification, at the vendor's cost.

7.4.8 **Procedural adherence:** All arming and disarming procedures shall be strictly followed.

7.4.9 **Supply options:** Sale, lease, and rental options shall be available but irrespective of the contracting mode adopted, the Vendor shall retain responsibility to KRA for seal accountability including live location tracing, prevention of misuse or unauthorized use and device decommissioning as may be directed by KRA. Vendors shall be accountable for losses suffered where revenue losses occur due to negligence over seal accountability and management.

7.4.10 **Risk management:** Vendors shall provide appropriate risk mitigation strategies including but not limited to insurance cover acceptable to KRA for indemnification against losses that may be occasioned by vendor negligence.

7.4.11 **Service continuity:** Vendors shall ensure uninterrupted service to contracted clients and arrange seamless subcontracting where necessary.

7.4.12 **Governing instruments:** Implementation shall be governed by the contract, applicable SOPs, and MoUs, as amended from time to time.

7.4.13 **Penalties:** Where penalties are not specified in the contract, provisions of the EAC CMA, 2004 shall apply.

7.4.14 **Conflict of laws:** In case of conflict, the EACCMA, 2004 shall prevail.

7.4.15 **Work experience:** Vendors must demonstrate evidence of prior experience in handling similar vehicular and/or cargo tracking operations for public or private entities at a scale of not less than one thousand (1,000) units.

8. TECHNICAL SPECIFICATIONS AND COMPLIANCE

Service Provider Vendors shall complete the compliance matrix below. Failure to complete Column (c) shall result in **automatic disqualification**.

8.1 Specific Technical Requirements

i. The seal should be able to attach to a container firmly and be able to withstand rough terrain conditions. Bidder must demonstrate the seal functionalities including but not limited to integration with vertical sensor, light sensor to validate Electronic Seal is correctly attached on container before arming and disarming via RFID card/biometric.

ii. Demonstrate from the previous clients where the bidder has installed Electronic Fuel Seal and are operational

iii. Other than Position tracking & route monitoring, the Electronic Fuel Seal must have the capability monitor all fuel types, fuel level, fuel density as well as auto detect any 5% or more of sudden level change in real time basis. It must also able to be armed and disarmed using RFID card via 4G/3G/EDGE/GPRS/GSM and WiFi and Bluetooth wireless connectivity to RECTS Platform, Store at least a total of 10,000 positioning and event data when there is no wireless connectivity available and upload it later to the RECTS Platform when wireless network is available.

iv. The Electronic Seal should be an integrated telematics terminal that can be programmed as per customs process(es) automation on KRA request. The device must be able to remotely detect any non-compliance and send real time alert to RECTS Platform.

v. Must demonstrate that seal can send alert when:

   a. There is seal tamper
   b. Unauthorized attempt/opening of the container.
   c. Arming devices are compromised
   d. The seal removed from geo-fenced route or area
   e. Excess idle time occurs due to prolonged stoppage;
   f. Accident event is detected

g. Seal activated or de-activated at unauthorized area or unauthorized person
h. Electronic Seal is detached from the container
i. interference with the Electronic Seal Cable/lock
j. Offroute

8.2 Detailed Technical Specifications

The following are the detailed technical specifications for each category of seal to be quoted:

8.2.1 Electronic Seal should be suitable for real time monitoring and tracking of high-risk consignments and should incorporate wireless connectivity like WIFI and Bluetooth.

8.2.1.1 The seal should have Sixty days battery life with continuous 5 mins interval tracking without external power as appropriate with electromagnetic induction capabilities.

8.2.2 Electronic Fuel Seal for real time fuel level monitoring and continuous 5 mins interval tracking of petroleum, ethanol and other high value liquids consignments.

ITEM NO.	***NAME OF GOODS OR RELATED SERVICE***	***TECHNICAL SPECIFICATIONS AND STANDARDS***	***VENDOR'S RESPONSE***
1	***eSEALS.***	*a) The warranty of the Electronic Seal should be minimum 18 months against manufacturer's defect.*	
		b) ***Primary Device Connectivity*** *All tracking devices shall establish a direct connection to the EAC RECTS server using the approved device communication protocol.* *The connection shall support secure, real-time data transmission between the device and the EAC RECTS server.* ***Vendor Telematics System Integration*** *All vendor telematics tracking systems may be integrated with the EAC RECTS platform.* *The integration shall enable automatic transmission and synchronization of tracking data from the EAC RECTS system to the Vendor systems as secondary data storage.* *The integration shall comply with the*	

		prescribed EAC RECTS interface specifications, data formats, and communication protocols.	
		c) Electronic Seals should offer a minimum of 60 days continuous tracking at every 5 mins interval and shall be fitted with a high-capacity battery, which may including electromagnetic induction capability to support charging while in motion.	
		d) The battery casing shall be marked with full KRA Corporate colour with logo	
		e) The Electronic Seal shall be able to attach to the container firmly and be able to withstand rough terrain conditions and not easily break during transit	
		f) The Electronic Seal design shall comply with IP 67 to provide a degree of protection against the entry of water during temporary submersion at a limited depth	
		g) Ability to withstand tropical conditions and rough terrain	
		h) The electronic seal shall be uniquely identifiable and readable with OCR/QR code technology or any other suitable technology for seal visibility in the system	

		i) The Electronic Seal shall be tamper proof and should generate alerts in case there is seal tamper or unauthorized activity.	
		j) The Electronic Seals shall have printed QR code/Optical Character Recognition (OCR) on the Electronic Seal label, which will be integrated with the Customs systems. Arming and disarming to be done by Custom Officer RFID after scanning the QR code/OCR the Electronic Seal ID printed on the Electronic Seal Label sticker, on the Electronic Seal casing, and status updated in RECTS System Software and respective customs system in the Region on real time basis	
		k) The Electronic Seal cable connector must be embedded with unique electronic ID.	
		l) The Electronic Seal must be able to automatically turn off all inbuilt wireless transceivers when located in a designated zone with no wireless transmission as per safety requirement.	
		m) The Electronic Seal must have alternative wireless connectivity so that it can transmit via WiFi or Bluetooth Network in the event Cellular Network coverage is not	

		available	
		n) The Electronic Seal must be light weight and portable not exceeding 1000g	
		o) Must Have embedded RFID reader to detect Custom Officer RFID for arming and disarming. The seal shall also be fitted with a lockable seal cable that can only be opened or detached by authorised Customs personnel, either remotely or through approved biometric authentication	
		p) The Electronic Seal should be capable of recording incidents when out of network coverage and transmitting them to RECTS Command Centre(s). when the network is available	
		q) The Electronic Seals should seamlessly and directly report to EAC RECTS Comm Servers	
		r) The eseal must have mechanism to prevent unauthorized arming and detect unauthorized device use.	
		s) The eseal shall be compliant with EAC RECTS operational standards	

		t)All eseals shall undergo piloting, testing, and validation for a minimum period of three (3) months to confirm accuracy, reliability, and compatibility with existing EAC RECTS platform.	
2.	***Electronic Fuel Seal***	*a) The Electronic Fuel Seal will be used for tracking Liquids under Customs control, including Ethanol and Petroleum Products, crude palm oil and Heavy Oil products conveyed by tankers. The tankers will have between 1 to 9 compartments. In addition to the normal Electronic eSeal functionality and alerts, the Electronic Fuel Seal shall monitor the volumes of fuel loaded, fuel discharged and location of discharge (send alert if volume change is detected in unauthorized location), and changes in density and volumes during transit. The measurement of the fuel level must have the accuracy of 2mm or better.* *The Detailed Technical Specifications for Electronic Fuel Seal are as follows:*	
		i) The warranty of the Electronic Fuel Seals should be 18 months against manufacturer's defect.	
		ii) ***Primary Device Connectivity*** *All tracking devices shall establish a direct connection to the EAC RECTS*	

		server using the approved device communication protocol. *The connection shall support secure, real-time data transmission between the device and the EAC RECTS server.* ***Vendor Telematics System Integration*** *All vendor telematics tracking systems shall be integrated with the EAC RECTS platform.* *The integration shall enable automatic transmission and synchronization of tracking data from the EAC RECTS system to the Vendor systems as secondary data storage.* *The integration shall comply with the prescribed EAC RECTS interface specifications, data formats, and communication protocols.*	
		iii) The Sensors must be attached externally on the tank. There should be no drilling, modification of the fuel tanks or insertion of any parts of the sensors into the tank in line with EPRA requirements.	
		iv) Fuel being highly flammable, the sensors should be safe for use, and must conform to international safety	

		standards	
		v) The Electronic Fuel Seal must be suitable for tracking either Ethanol and Petroleum Products, crude palm oil and Heavy Oil products and any other liquids under Customs control	
		vi) The Electronic Fuel Seal must have an accuracy of at least 2mm or better on the fuel level for each of the compartments,	
		vii) The sensors must have capability to continuously monitor the liquid levels in all compartments of the Tanker	
		i) The tracking must give an accuracy of not more than 2 metres of the actual position of the tanker	
		j) The controller Must be permanently installed in tanker trucks chassis	
		k) The Electronic Fuel Seal must withstand tropical conditions and rough terrain	
		l) The Electronic Fuel Seals should be uniquely identifiable using QR code/Optical Character Recognition (OCR) or such other suitable technology, on the Electronic Fuel Seal label, which will be integrated with the Customs systems.	

		m) Arming and disarming of the Electronic Fuel Seal shall be done by Custom Officer using RFID by scanning the Electronic Fuel Seal ID and status updated in RECTS Command Centre(s) Software in sync with the respective Customs Systems	
		n) The Electronic Fuel Seal must have alternative wireless connectivity so that it can transmit via WiFi or Bluetooth Network in the event Cellular Network coverage is not available	
		o) The Electronic Fuel Seal must be able to automatically turn off all inbuilt wireless transceivers when it is located in a designated zone with no wireless transmission as per safety requirements.	
		p) The Electronic Fuel Seal shall seamlessly and directly report to the EAC RECTS Comm Servers	
3.	***eSEAl Logistics service***	*The vendor shall have the capability and capacity of providing the following seal logistics services*	
		a) Collection of the Electronic eSeals from the all exit/ destination Customs offices in the partner states.	
		b) Transportation and delivery of the Electronic Seals to the designated arming points.	

4.	***Repair and Maintenance of the seals***	*The vendor shall have maintenance centres for repairs and QA services.* *Maintenance includes the following.* *a) Cleaning of the Electronic Seals/Electronic Fuel Seals*	
		b) Testing, and upgrading of the firmware	
		c) Validation of the Electronic Seals/Electronic Fuel Seal	
		d) Quality assurance of the Electronic Seals/Electronic Fuel Seals, Charging of the Electronic Seal	
		e) Service Provider Vendor shall be responsible for 100% precheck with proof before devices are sent for arming	
		f) Services Provider Vendor must assure Devices are fully charge (at least capable to reporting throughout the journey up to 60 days) before sending for arming.	
		g) Provide adequate stock levels of Electronic Seal/Electronic Fuel Seal consumables	
		h) Service Provider Vendor shall not charge Transporter unless it is proven the devices were tampered or mishandled.	

5.	***Delivery Schedule***	*Successful Service Vendors should be able to deliver the first batch (60%) of seals within 50 days and the balance within 90 days upon approval.*	

8.3 Business and Operation Requirements Compliance

8.3.1 Service Vendors shall demonstrate institutional capacity, regulatory compliance, and commercial independence as follows:

i. Demonstrated experience in implementing **similar large-scale tracking solutions** for public or private sector entities, involving **a minimum of 1,000 tracking units**.

ii. Proven availability of **regional support resources across the entire East African Community (EAC)**, with specific operational presence in Kenya at:

   a. Port of Mombasa
   b. Container Freight Stations (CFS)
   c. Inland Container Depots (ICDs)
   d. Customs Bonded Warehouses (CBWHSE)
   e. Land Border Stations
   f. Any other Customs-controlled areas as may be designated by KRA.

iii. Availability of **repair and maintenance facilities** capable of servicing **at least 1,000 Seals**, located within reasonable proximity to key Customs operational hubs, including **Mombasa, Nairobi, and major Kenyan border points**.

iv. Submission of a **comprehensive business plan** detailing implementation strategy, operational model, staffing, logistics, financial sustainability, and resource commitments.

v. Possession of a valid **Communications Authority of Kenya (CAK) license** authorizing the sale, servicing, and maintenance of the relevant category of electronic tracking equipment.

vi. Demonstrated compliance with **Kenyan tax laws and statutory obligations**, including **but not limited to** submission of valid tax compliance certificates.

8.3.2 Vendors shall demonstrate the operational capacity to support continuous, nationwide deployment of EAC RECTS services, including:

i. Capacity to supply and maintain a **minimum of 1,000 serviceable Seals**, together with the full suite of services specified in the Schedule of Requirements.

ii. Deployment of adequately trained personnel and supporting resources at **all arming and disarming stations**, including:
   a. Mombasa Port
   b. Container Freight Stations
   c. Inland Container Depots
   d. Customs Bonded Warehouses
   e. Land Border Stations
   f. Any other Customs-controlled areas as may be specified by KRA.

iii. Ability to position and manage a **specified number of Seals at designated Customs locations**, currently numbering **one hundred and fifty-five (155)**, as detailed in the relevant schedule, and to provide the logistical resources required for activation, deactivation, collection, and transportation of seals to and from central arming points.

iv. Vendor operations shall be available for 24 hours at all locations.

v. Strict adherence at all times to **approved arming and disarming operational procedures**.

vi. Timely provision of electronic eseal services to all contracted clients. Where service disruption is anticipated, Vendors shall make **prior, seamless arrangements** to ensure business continuity without jeopardizing operations.

8.4 Services Level Agreements

SCOPE OF SERVICES

8.4.1 Inventory Managed Service

Inventory Managed Services include the following;

a. Collection of the Seals from the place of disarming.
b. Secure packaging of the Seals in specialized boxes/ cases to ensure seals are not damaged during transportation.
c. Transportation and delivery of the Seals to the maintenance centers.
d. Distribution of Seals to the arming locations.
e. Use of tools that support OCR/QR code reader to ensure efficient and accurate data capture.
f. Provision of accurate records for the seals in the whole logistic chain.
g. Record keeping of location of all Seal.
h. Provide seal location visibility irrespective of the seal status.

8.4.2 Repair and Maintenance of the Electronic Seals/Electronic Fuel Seals

Maintenance services includes the following:

a. Cleaning of the Electronic Seals/Electronic Fuel Seals.
b. Detailed inspection of the Electronic Seals/Electronic Fuel Seals.
c. Testing, and upgrading of firmware.
d. Validation of the Electronic Seals/Electronic Fuel Seal.
e. Quality Assurance (QA) of the Electronic Seals/Electronic Fuel Seals.
f. Charging of the Electronic Seal.
g. Repair of faulty Electronic Seals/Electronic Fuel Seals.
h. Provide secure storage of Electronic Seals while under repair and maintenance.
i. Dispatch of Electronic Seals after repair and maintenance.
j. Provide adequate stock levels of Electronic Seal/Electronic Fuel Seal consumables.

8.4.3 SEAL AVAILABILITY, ACCOUNTABILITY AND TIMELY COLLECTION

The Vendors shall ensure:

8.4.3.1 Availability of e-seals at all arming stations and observe defined minimum inventory levels (see table 4: Minimum Stock Levels)

8.4.3.2 Accountability of all e-seals by providing seals visibility irrespective of their status as defined below:

a. Devices under circulation
b. On transit (activated)
c. Journey completed (Deactivated)
d. Location after deactivation
e. Return inwards: Movement from deactivation location to MO
f. Receipt at MO

8.4.3.3 Timely collection and distribution of seals

8.4.4 KEY PERFORMANCE INDICATORS

The following are the key performance indicators

S/No.	KPI	No	Target
1	Ensure availability of minimum eSEALs stocks at all arming stations	1000	100%
2	Seal in good working condition with all accessories	1000	97%
3	Timely collection and distribution of eSEALs	1000	98%
4	Ensure eSEAL accountability at all times (eFUEL/ eSEAL)	1000	98%

Table 1: Key Performance Indicators

8.4.5 SEAL MANAGEMENT FRAMEWORK

The following rules will be applied in the management of Seals;

8.4.5.1Arming/ Disarming of the Seals will be done at the arming and disarming Station as per EAC RECTS SOPs (Annex 1). However, for ease of seal management the following rules shall be implemented in the system.

a. All KRA Vendor eSeals shall only be armed within Kenya or in a Partner States for cargo destined to Kenya or Transiting through Kenya,

8.4.5.2 The Vendors shall ensure that all disarmed eSeals are collected and delivered to their maintenance and distribution centres.

8.4.5.3 The Vendors shall ensure the Seals are in good working condition before distribution to the arming stations.

8.4.5.4 The Vendors shall distribute the Seals to stations as per the SLA, monitor usage and replenish them to maintain the required minimum stock levels.

8.4.6 MINIMUM STOCK LEVELS TO BE MAINTAINED AT CUSTOMS STATION

S/no	Customs Station	Minimum Stock levels
1.	Isebania Customs Station	50
2.	Loitoktok Custom Station	50
3.	Namanga Customs Station	100
4.	Taveta Custom Station	100
5.	EPZ Athi River Zone	50
6.	EPZ Sameer Park	50
7.	Mombasa Port	1000
8.	Nairobi Inland Container Depot ICD	200
9.	Lunga Lunga	50
10.	Malaba	100
11.	Busia	50
12.	Naivasha Inland Container Depot ICD	100
	Total	**1850**
NB: Malaba and Busia are mainly exit stations, arming for most incoming cargo will be done by the Partner States respectively. On special occasions arming might be required.		

Table 2: Minimum Stock Levels

8.4.7 INCIDENT MANAGEMENT AND SUPPORT

8.4.7.1 The Vendors shall establish maintenance offices to respond to incidences and support requests by KRA staff. The Vendors shall endeavour to respond to all reported incidences within 30 minutes and issue a report back to the contact person.

8.4.7.2 The incidents/ Support requests will be done by mail and once resolved, a confirmation email to close the issue be done.

8.4.7.3 Chief Manager responsible for Cargo Monitoring or his appointed officer will be the contact person for KRA

8.4.8 MONITORING AND EVALUATION

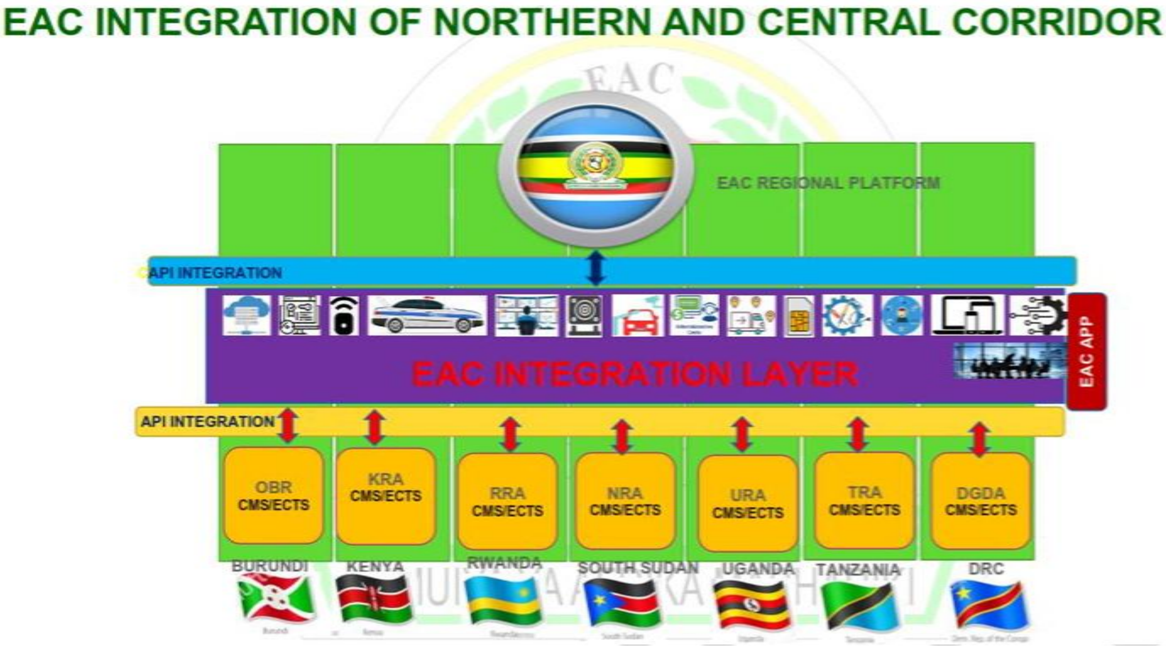
8.4.8.1 The Chief Manager Cargo Monitoring Unit will be responsible to ensure adherence of the provisions of this SLA at all times.

8.4.8.2 Review meeting will be held monthly with the Services Provider Vendors to monitor progress and a joint report signed.

8.4.10 TERMINATION CLAUSE.

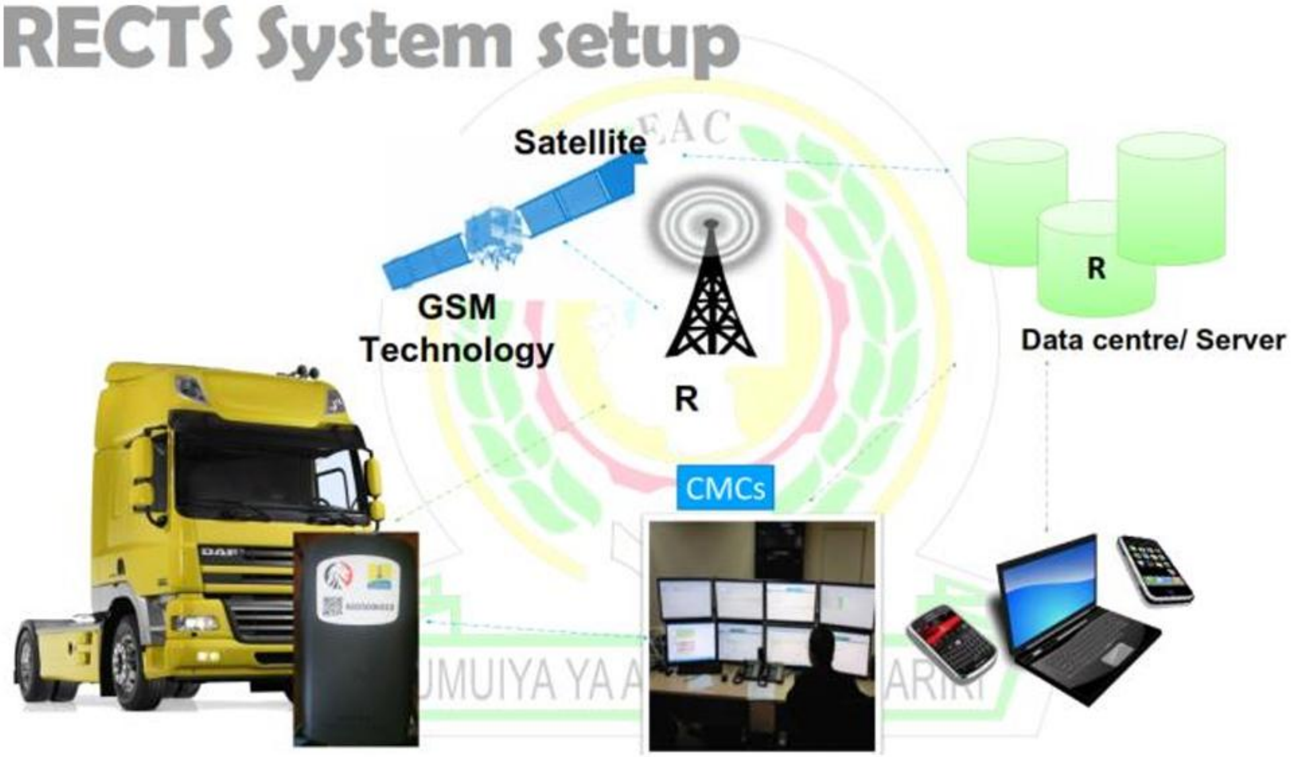
8.4.10.1 The Vendors shall be terminated for failure to comply with the SLA.

Proposed Model Diagram of the Common Platform



(A more robust and cost effective technology is acceptable provided that it can send the specified information to the KRA RECTS)

NOTE: KRA reserves the right to change the model in event it shall be proved to produce unsatisfactory performance



Integration Logical flow diagram

9. ROLES AND RESPONSIBILITIES

9.1 Kenya Revenue Authority (KRA)

In the multi-vendor user owned eseal framework KRA shall be responsible for overall governance and regulatory oversight in the EAC RECTS, including:

- Registration of all approved electronic devices, including **Electronic Seals, Electronic Fuel Seals, Electronic Lock Seals, and Electronic Net Seals**, for each qualified Vendor.
- Inspection and approval of seal installation prior to operational use.
- Continuous monitoring of vendor compliance with contractual, technical, and statutory requirements.
- Real-time monitoring of cargo movements under customs control.
- Operation and maintenance of EAC RECTS infrastructure, including control room and server facilities.
- Loading of cargo and journey information into electronic seals at the point of journey initiation and activation of the devices.
- Deactivation of electronic eseals upon confirmation of actual arrival of goods at the destination, followed by formal notification to the Vendor to disarm the seal.

9.2 Cargo Transporters

Cargo Transporters shall be responsible for operational compliance during transit, including:

- Procuring **KRA-registered eseals** from approved Vendors.
- Ensure the vendor has presented a registered electronic seals to KRA at the **Journey Initiation Point** for loading of cargo information and activation.
- Maintaining the integrity and functionality of eseals during transit and reporting any defects or damage immediately.
- Installing permanent **Electronic Fuel Seal Sensors** on petroleum tankers and ensuring proper installation, calibration, and maintenance.

- Adhering strictly to **geo-fenced gazette transit routes**.
- Providing training to drivers on the proper use, maintenance, safety, and security of electronic seals.
- Reporting damaged or malfunctioning equipment to the Vendor for repair, replacement, or recalibration.
- Immediately notifying KRA of any incident that may impair seal functionality, including accidents, theft, or tampering.

9.3 Customs Agents

Customs Agents shall support compliance and continuity of operations by:

- Ensure the vendor has presented a registered electronic seal to KRA at the **Journey Initiation Point** for loading of cargo information and activation.
- Maintaining electronic seals on vehicles moving on their own wheels and reporting any defects or damage during transit.
- Ensuring movement strictly along **geo-fenced gazette routes**.
- Reporting damaged equipment to the relevant Vendor for corrective action.
- Immediately informing KRA of any incident that may render a seal inoperative or unreliable.

9.4 Approved Vendors

Approved Vendors shall be responsible for the supply, operation, and lifecycle management of electronic seals, including:

- Registration and provision of all electronic seals intended for use by Transporters with KRA.
- Payment of all GPS/GPRS communication charges associated with device operation.
- Provision of maintenance, repair, charging, calibration, and quality assurance services for all devices.
- Periodic notification to KRA regarding availability of new or improved seal technologies.

- Ensuring **24/7 service availability** across all operational locations.
- Full compliance with KRA-prescribed technical standards and system integration protocols, including adherence to the communication protocol outlined in **Appendix (i)**.
- Submission of device samples to KRA for registration and quality assurance, submitted samples will be retained for reference purposes.
- Provision of operational training on electronic seals to KRA Customs officers when required.

EVALUATION CRITERIA

No.	Criterion	Marks
1	Self-Financing Business Plan	5
2	Technical Performance (≥95%)	60
3	System Integration Capability	5
4	Financial Capacity (≥1,000 seals)	5
5	Regional Operational Resources	5
6	Regional Logistics Capability	5
7	Experience and Technical Personnel	5
8	Annual Turnover ≥ KES 300 Million	5
9	References / Manufacturer Support	5
Total	**Minimum Qualifying Score**	**100**

11. MULTI VENDOR USER OWNED ESEALS FRAMEWORK GOVERNANCE AND OVERSIGHT

11.1 Confidentiality

All information exchanged under this qualification framework shall be treated as confidential. Vendors shall not disclose any operational or technical information without prior written approval of KRA.

11.2 Audit and Compliance Rights

KRA reserves the right to conduct audits, inspections, and compliance verification of Vendor operations, seals, systems, financial records, and regional support facilities at any time during the framework period.

11.3 Disqualification and Suspension

KRA may suspend or disqualify any Vendor found to have:
(a) Provided false information,
(b) Fails to meet SLA,
(c) Engaged in collusion or conflict of interest,
(d) Compromises integrity of cargo monitoring operations.

11.4 Multi-Vendor Allocation Rules

KRA may allocate seal service volumes among qualified Vendors to ensure continuity, fairness, and operational trasparency, including phased onboarding for SCT and duty-paid cargo.

11.5 Regional Recognition and Partner State Governance

Implementation shall be governed by EAC RECTS policies, applicable MoUs, and mutual recognition arrangements among Partner States.

13. APPENDICES

Appendix I: Communication Protocol Guidelines

Communication Protocol Guidelines

Overview of ESEAL/EFUEL SERIES OVER-THE-AIR Communication

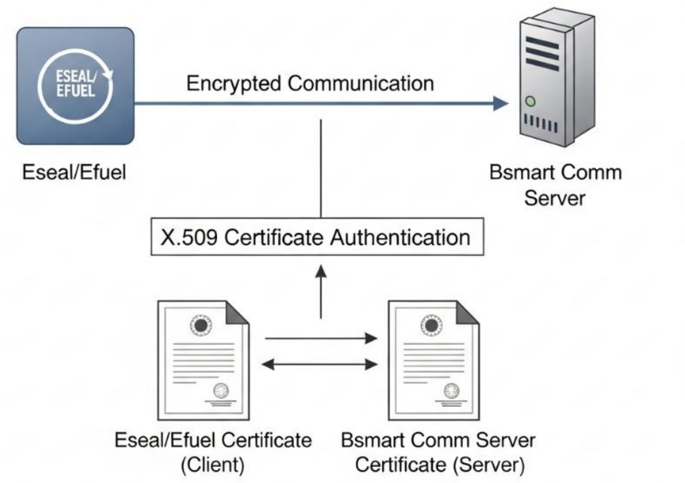
The RECTS eSEAL / eFUEL system is an integrated IoT solution designed for secure seal management, fuel monitoring, and regulatory data reporting.

The system enables field devices to transmit operational data to central server platforms using both TCP and HTTP REST communication protocols, ensuring reliability, flexibility, and network adaptability across different deployment environments.

Both protocols are designed to carry the same unified JSON payload structure, allowing consistent data processing on the server side regardless of the transport mechanism.

Communication Architecture

The RECTS integration architecture supports dual uplink communication paths from device to server with encrypted TCP-based data reporting,


ESEAL/ EFUEL
Encrypted Communication
Eseal/Efuel
Bsmart Comm Server
X.509 Certificate Authentication
Eseal/Efuel Certificate (Client)
Bsmart Comm Server Certificate (Server)

TCP Protocol (Persistent Data Channel)

The TCP protocol provides a persistent, connection-oriented channel for device data transmission.

Key Characteristics

- Long-lived TCP connections
- TLS or mutual TLS (mTLS) encryption
- Low-latency and reliable delivery
- Efficient for frequent or continuous data reporting

Payload Model

JSON data model is adopted in the payload formation with following benefits:

- Consistent data interpretation
- Unified server-side validation and processing logic
- Simplified protocol maintenance and versioning
- Seamless switching between transport mechanisms

Device Authentication and encryption

To guarantee the security of our communication, we employ X.509 certificate authentication. This method provides strong mutual authentication between the eFuel/eSeal/eLock devices and the Comm Server. Each device and the server possess unique digital certificates issued by RECTS operation. During the connection handshake, these certificates are exchanged and verified, ensuring that only authorized entities can establish communication. This approach effectively prevents unauthorized access and man-in-the-middle attacks, safeguarding the sensitive data transmitted between our devices and the platform

On top of that, the Electronic Seal must be integrated with ECTS enabled Blockchain to validate the encrypted off-chain command with ECTS Device Smart Contract Registry to perform (but not limited to) Activation/Deactivation procedure.

Domain Name–Based Server Resolution

To avoid dependency on fixed IP addresses, eFuel,eSeal,eLock devices are configured to use domain names (DNS) to identify backend servers.

- Devices store backend endpoints as fully qualified domain names (FQDNs).

- During connection establishment, the device resolves the domain name to obtain the current server IP address.
- This design allows backend server IP addresses to change due to maintenance, scaling, or infrastructure migration without requiring firmware updates or device reconfiguration.
- Using DNS-based resolution ensures long-term flexibility and reduces operational risk in dynamic infrastructure environments.

Multi-Server Configuration and Automatic Failover

In addition to DNS-based resolution, eFuel,eSeal,eLock devices support configuration of multiple backend servers to ensure service continuity in case of server unavailability.

- Devices maintain a prioritized list of backend servers, each identified by a domain name.
- The primary server is used under normal operating conditions.
- If connection attempts to the primary server fail due to timeout, network error, or service unavailability, the device automatically attempts to connect to secondary or fallback servers.
- Failover is handled internally by the device firmware and requires no external intervention.

This mechanism ensures uninterrupted data transmission, command reception, and monitoring even during backend outages.

Device reporting events

Overview

This chapter defines the unified device reporting framework for the RECTS eSEAL and eFUEL systems.

Both device types use a common reporting architecture and payload model, enabling consistent data ingestion, auditing, and regulatory supervision while serving different operational domains.

The reporting mechanism is designed to support customs control, cargo security, fuel accountability, and energy auditing, in alignment with government and regulatory requirements.

Reporting Scope

The RECTS device reporting framework covers three major categories:

1. Regular Operational Reporting
2. Event-Based Reporting
3. Alert and Exception Reporting

These categories apply consistently to both eSEAL and eFUEL devices, ensuring standardized handling and prioritization across the platform.

Report data payloads

Overall data payload model

Field Name	Description	Required	
latitude	Latitude (in decimal degrees)	Yes	decimal degrees
longitude	longitude (in decimal degrees)	Yes	decimal degrees
altitude	Altitude	Yes	Integer
timestamp	GPS Time stamp in milliseconds	Yes	Long
speed	Speed (km/h)	Yes	decimal degrees
bearing	Direction (degree)	Yes	decimal degrees
satellite	Receivable Number of satellites	Yes	Integer

count			
HDOP	Horizontal Dilution Of Precision (Quality of GPS signal)	Yes	decimal degrees
d2d3	Satellite mode 2D or 3D	Yes	2 or 3
RSSI	Received Signal Strength Indication	Yes	integer
LAC	Local Area Code	Yes	integer
Cell_ID	Cell ID	Yes	integer
MCC	Mobile Country Code	Yes	integer
MGS_ID	Unique data running number (64bits)	Yes	integer
Activity_id	Activity ID for the message, see Activity Message Description	Yes	integer
addon_info	Add-on information for related activity in JSON format depends on the activity ID	Optional	addon_info
fuel_info	Fuel data information object when activity id is 12(activity = 12)		fuel_info

Example for Activity 1 GPS reporting:

```
{
  "latitude": "-6.79124",
  "longitude": "39.1",
  "altitude": "21",
  "timestamp": "1541603095967",
  "horizontal_speed": "80",
  "vertical_speed": "0",
  "bearing": "150",
  "satellite_count": "9",
  "HDOP": "1",
  "d2d3": "3",
  "RSSI": "0",
  "LAC": "123",
  "Cell_ID": "12345",
  "MGS_ID": "12345",
  "MCC": "635",
  "activity_id": "001"
}
```

Activity Messages

Activity ID: 001 – Movement / Logging

Activity Name	Movement / Logging
Activity Category	Regular Reporting
Description	Periodic logging of GPS position, speed, direction, and device status during transit.
Trigger Condition	Device operating normally within reporting interval.
Device Functionality	Collects GPS and operational data.
Severity Level	Informational
Regulatory Impact	Trip traceability
Applicable Device	eSeal,eFuel,eLock

Activity ID: 002 – Fuel Data Reporting

Activity Name	Fuel Data Reporting
Activity Category	Event
Description	Regular reporting of fuel level and sensor health data.
Trigger Condition	Scheduled fuel reporting interval.
Device Functionality	Reads fuel sensor and transmits data.
Severity Level	Informational
Regulatory Impact	Fuel accountability
Applicable Device	eFuel

Activity ID: 003 – Enter Checkpoint

Activity Name	Enter Checkpoint
Activity Category	Event
Description	Device enters predefined checkpoint or geofence.
Trigger Condition	GPS enters checkpoint boundary.

Device Functionality	Detects geofence entry.
Severity Level	Informational
Regulatory Impact	Customs compliance
Applicable Device	eFuel

Activity ID: 004 – Leave Checkpoint

Activity Name	Leave Checkpoint
Activity Category	Event
Description	Device exits predefined checkpoint or geofence.
Trigger Condition	GPS exits checkpoint boundary.
Device Functionality	Detects geofence exit.
Severity Level	Informational
Regulatory Impact	Transit compliance
Applicable Device	eFuel

Activity ID: 005 – Fuel Loading Detected

Activity Name	Fuel Loading Detected
Activity Category	Event
Description	Normal fuel loading activity detected.
Trigger Condition	Fuel level increases beyond threshold.
Device Functionality	Detects fuel increase.
Severity Level	Informational
Regulatory Impact	Fuel audit
Applicable Device	eFuel

Activity ID: 006 – Fuel Offloading Detected

Activity Name	Fuel Offloading Detected
Activity Category	Event
Description	Normal fuel offloading activity detected.
Trigger Condition	Fuel level decreases beyond threshold.
Device Functionality	Detects fuel decrease.
Severity Level	Informational
Regulatory Impact	Fuel audit
Applicable Device	eFuel

Activity ID: 007 – GPS Signal Not Available

Activity Name	GPS Signal Not Available
Activity Category	Alert
Description	GPS signal loss detected.
Trigger Condition	No GPS fix for configured duration.
Device Functionality	Monitors GPS module status.
Severity Level	Warning
Regulatory Impact	Tracking continuity
Applicable Device	eSeal,eFuel,eLock

Activity ID: 008 – Speeding

Activity Name	Speeding
Activity Category	Alert
Description	Vehicle exceeds configured speed limit.
Trigger Condition	Speed above threshold (eg > 80km/h).
Device Functionality	Monitors speed.
Severity Level	Warning
Regulatory Impact	Road safety
Applicable Device	eSeal,eFuel,eLock

Activity ID: 009 – Harsh Braking

Activity Name	Harsh Braking
Activity Category	Alert
Description	Sudden deceleration detected.
Trigger Condition	Acceleration below braking threshold.
Device Functionality	Uses accelerometer.
Severity Level	Warning
Regulatory Impact	Driver behavior
Applicable Device	eFuel

Activity ID: 010 – Harsh Turning

Activity Name	Harsh Turning
Activity Category	Alert
Description	Sharp turning detected.

Trigger Condition	Lateral acceleration exceeds limit.
Device Functionality	Monitors accelerometer.
Severity Level	Warning
Regulatory Impact	Driver behavior
Applicable Device	eFuel

Activity ID: 011 – Harsh Acceleration

Activity Name	Harsh Acceleration
Activity Category	Alert
Description	Rapid acceleration detected.
Trigger Condition	Acceleration above threshold.
Device Functionality	Monitors accelerometer.
Severity Level	Warning
Regulatory Impact	Driver behavior
Applicable Device	eFuel

Activity ID: 012 – Internal Battery Low

Activity Name	Internal Battery Low
Activity Category	Alert
Description	Internal battery below warning level.
Trigger Condition	Voltage below warning threshold. (battery < 30%)
Device Functionality	Monitors battery.
Severity Level	Warning
Regulatory Impact	Device availability
Applicable Device	eSeal,eFuel,eLock

Activity ID: 013 – Internal Battery Critical Low

Activity Name	Internal Battery Critical Low
Activity Category	Alert
Description	Internal battery critically low.
Trigger Condition	Voltage below critical threshold (battery < 15%).
Device Functionality	Enters power saving for Eseal/Elock.
Severity Level	Critical
Regulatory Impact	Device continuity

Applicable Device	eSeal,eFuel,eLock

Activity ID: 014 – Battery Level Excessively High

Activity Name	Battery Level Excessively High
Activity Category	Alert
Description	Battery voltage abnormally high.
Trigger Condition	Voltage exceeds max threshold.
Device Functionality	Detects abnormal voltage.
Severity Level	Warning
Regulatory Impact	Battery safety
Applicable Device	eSeal,eFuel,eLock

Activity ID: 015 – Internal Battery Disconnected

Activity Name	Internal Battery Disconnected
Activity Category	Alert
Description	Internal battery disconnected.
Trigger Condition	Battery circuit open.
Device Functionality	Detects disconnection.
Severity Level	Critical
Regulatory Impact	Device tamper
Applicable Device	eFuel

Activity ID: 016 – External Power Supply Low

Activity Name	External Power Supply Low
Activity Category	Alert
Description	External power supply voltage low (<9V).
Trigger Condition	External voltage below threshold.
Device Functionality	Monitors power input.
Severity Level	Warning
Regulatory Impact	Power stability
Applicable Device	eFuel

Activity ID: 017 – External Power Disconnected

Activity Name	External Power Disconnected
Activity Category	Alert

Description	External power disconnected from device.
Trigger Condition	Loss of external power.
Device Functionality	Detects power loss.
Severity Level	Warning
Regulatory Impact	Power continuity
Applicable Device	eFuel

Activity ID: 018 – Accident / Rollover

Activity Name	Accident / Rollover
Activity Category	Alert
Description	Rollover or severe impact detected.
Trigger Condition	Acceleration exceeds impact threshold.
Device Functionality	Detects via accelerometer.
Severity Level	Critical
Regulatory Impact	Safety incident
Applicable Device	eSeal,eFuel,eLock

Activity ID: 019 – Device Tampering

Activity Name	Device Tampering
Activity Category	Alert
Description	Unauthorized device tampering detected.
Trigger Condition	Casing or sensor tamper switch triggered.
Device Functionality	Detects tamper.
Severity Level	Critical
Regulatory Impact	Security breach
Applicable Device	eSeal,eFuel,eLock

Activity ID: 020 – Off Route

Activity Name	Off Route
Activity Category	Alert
Description	Device deviates from planned route.
Trigger Condition	GPS outside allowed corridor.
Device Functionality	Monitors route compliance.
Severity Level	Warning

Regulatory Impact	Transit compliance
Applicable Device	eSeal,eFuel,eLock

Activity ID: 021 – Invalid NFC Scanned

Activity Name	Invalid NFC Scanned
Activity Category	Alert
Description	Invalid NFC tag scanned.
Trigger Condition	NFC UID not authorized.
Device Functionality	Validates NFC.
Severity Level	Warning
Regulatory Impact	Access control
Applicable Device	eSeal,eLock,eFuel

Activity ID: 022 – RFID Card Not Registered

Activity Name	RFID Card Not Registered
Activity Category	Alert
Description	Unregistered RFID card used.
Trigger Condition	RFID UID not in whitelist.
Device Functionality	Validates RFID.
Severity Level	Warning
Regulatory Impact	Access control
Applicable Device	eSeal,eLock

Activity ID: 023 – Seal Broken – Procedure Error

Activity Name	Seal Broken – Procedure Error
Activity Category	Alert
Description	Seal cable/lock disconnected before proper deactivation.
Trigger Condition	Seal opened without procedure.
Device Functionality	Detects seal open.
Severity Level	Critical
Regulatory Impact	Customs violation
Applicable Device	eSeal

Activity ID: 024 – Seal Broken – Unauthorized Zone

Activity Name	Seal Broken – Unauthorized Zone
Activity Category	Alert
Description	Seal cable/lock opened outside authorized zone.
Trigger Condition	Seal open outside geofence.
Device Functionality	Detects seal open.
Severity Level	Critical
Regulatory Impact	Customs violation
Applicable Device	eSeal

Activity ID: 025 – Seal Cut Alert

Activity Name	Seal Cut Alert
Activity Category	Alert
Description	Seal cable cut detected.
Trigger Condition	Cable continuity lost.
Device Functionality	Immediate tamper alert.
Severity Level	Critical
Regulatory Impact	Cargo integrity
Applicable Device	eSeal

Activity ID: 026 – Seal Lock Error

Activity Name	Seal Lock Error
Activity Category	Alert
Description	Seal unable to lock properly.
Trigger Condition	Lock mechanism failure.
Device Functionality	Detects lock error.
Severity Level	Warning
Regulatory Impact	Operational reliability
Applicable Device	eSeal,eLock

Activity ID: 027 – Seal Unlock Error

Activity Name	Seal Unlock Error
Activity Category	Alert
Description	Seal cannot unlock.
Trigger Condition	Unlock mechanism failure.

Device Functionality	Detects unlock error.
Severity Level	Warning
Regulatory Impact	Operational reliability
Applicable Device	eSeal,eLock

Activity ID: 028 – Seal Detached

Activity Name	Seal Detached
Activity Category	Alert
Description	Seal detached from container.
Trigger Condition	Mounting sensor triggered.
Device Functionality	Detects detachment.
Severity Level	Critical
Regulatory Impact	Cargo security
Applicable Device	eSeal,eLock

Activity ID: 029 – Illegal Seal Activation

Activity Name	Illegal Seal Activation
Activity Category	Alert
Description	Seal activated without valid NFC.
Trigger Condition	Activation without authorization.
Device Functionality	Validates activation.
Severity Level	Critical
Regulatory Impact	Security breach
Applicable Device	eSeal,eLock

Activity ID: 030 – Illegal Seal Deactivation

Activity Name	Illegal Seal Deactivation
Activity Category	Alert
Description	Seal deactivated illegally.
Trigger Condition	Deactivation without authorization (or valid NFC scan).
Device Functionality	Validates deactivation.
Severity Level	Critical
Regulatory Impact	Security breach

Applicable Device	eSeal,eLock

Activity ID: 031 – Cross Country Alert

Activity Name	Cross Country Alert
Activity Category	Alert
Description	Device crosses national border unexpectedly.
Trigger Condition	Country code change detected.
Device Functionality	Monitors MCC/GPS.
Severity Level	Critical
Regulatory Impact	Customs enforcement
Applicable Device	eSeal,eFuel,eLock

Activity ID: 032 – Command Failure

Activity Name	Command Failure
Activity Category	Alert
Description	Failure executing OTA command.
Trigger Condition	Command validation/execution error.
Device Functionality	Aborts command.
Severity Level	Warning
Regulatory Impact	Audit trail
Applicable Device	eSeal,eFuel,eLock

Activity ID: 033 – Exceed Transit Duration

Activity Name	Exceed Transit Duration
Activity Category	Alert
Description	Transit duration exceeded.
Trigger Condition	Trip active beyond expected exit time. (Defined as trip_expected_time in smart contract)
Device Functionality	Monitors trip timer.
Severity Level	Warning
Regulatory Impact	Transit SLA
Applicable Device	eSeal,eFuel,eLock

Activity ID: 034 – Exceed Stop Duration

Activity Name	Exceed Stop Duration

Activity Category	Alert
Description	Vehicle stopped longer than allowed.
Trigger Condition	Stop duration exceeds threshold.
Device Functionality	Monitors speed/time.
Severity Level	Warning
Regulatory Impact	Operational compliance
Applicable Device	eSeal,eFuel,eLock

Activity ID: 035 – eFuel Casing Open

Activity Name	eFuel Casing Open
Activity Category	Alert
Description	eFuel casing opened.
Trigger Condition	Open the casing of the eFuel device.
Device Functionality	Detects tamper.
Severity Level	Critical
Regulatory Impact	Fuel security
Applicable Device	eFuel

Activity ID: 036 – eSeal Casing Open

Activity Name	eSeal Casing Open
Activity Category	Alert
Description	eSeal casing opened.
Trigger Condition	Open the casing of the eSeal device.
Device Functionality	Detects tamper.
Severity Level	Critical
Regulatory Impact	Security breach
Applicable Device	eSeal

Activity ID: 037 – eSeal Fully Charged

Activity Name	eSeal Fully Charged
Activity Category	Event
Description	eSeal battery fully charged.
Trigger Condition	Battery reaches full charge.
Device Functionality	Monitors charging.

Severity Level	Informational
Regulatory Impact	Maintenance
Applicable Device	eSeal

Activity ID: 038 – Fuel Sensor Hardware Error

Activity Name	Fuel Sensor Hardware Error
Activity Category	Alert
Description	Invalid or unsupported fuel sensor detected.
Trigger Condition	Plug unauthorized fuel sensor / Wrong Fuel sensor hardware detected.
Device Functionality	Validates sensor.
Severity Level	Critical
Regulatory Impact	Measurement accuracy
Applicable Device	eFuel

Activity ID: 039 – Fuel Sensor Detached

Activity Name	Fuel Sensor Detached
Activity Category	Alert
Description	Fuel sensor detached from tank.
Trigger Condition	Sensor connection lost.
Device Functionality	Detects disconnection.
Severity Level	Critical
Regulatory Impact	Fuel integrity
Applicable Device	eFuel

Activity ID: 040 – Fuel Sensor Disconnected

Activity Name	Fuel Sensor Disconnected
Activity Category	Alert
Description	Fuel sensor disconnected from eFuel.
Trigger Condition	Fuel sensor wiring cut/unplugged from eFuel.
Device Functionality	Detects signal loss.
Severity Level	Critical
Regulatory Impact	Fuel monitoring
Applicable Device	eFuel

Activity ID: 041 – Fuel Offloading Alert

Activity Name	Fuel Offloading Alert
Activity Category	Alert
Description	Abnormal fuel offloading detected.
Trigger Condition	Rapid fuel decrease.
Device Functionality	Analyzes trend.
Severity Level	Critical
Regulatory Impact	Fuel theft detection
Applicable Device	eFuel

Activity ID: 042 – Fuel Sensor Power Loss

Activity Name	Fuel Sensor Power Loss
Activity Category	Alert
Description	Fuel sensor power failure.
Trigger Condition	eFuel unable to power the fuel sensor (eg. shorted the power supply)
Device Functionality	Detects power failure.
Severity Level	Critical
Regulatory Impact	Fuel monitoring
Applicable Device	eFuel

Activity ID: 043 – Fuel Density Change Alert

Activity Name	Fuel Density Change Alert
Activity Category	Alert
Description	Fuel density abnormal change detected.
Trigger Condition	Density outside allowed range.
Device Functionality	Analyzes density.
Severity Level	Warning
Regulatory Impact	Fuel quality
Applicable Device	eFuel

Activity ID: 044 – 11-Hour Driving Limit

Activity Name	11-Hour Driving Limit
Activity Category	Alert

Description	Driving limit as per FMCSA regulation, that driving time for property-carrying vehicles can not exceed 11hrs after 10 hrs off duty.
Trigger Condition	Driving duration exceeds limit 11-hours
Device Functionality	Tracks driving time.
Severity Level	Warning
Regulatory Impact	Driver compliance (FMCSA)
Applicable Device	eFuel

Activity ID: 045 – 60 Hour / 7 Day Limit

Activity Name	60 Hour / 7 Day Limit
Activity Category	Alert
Description	Driving limit as per FMCSA regulation, that driving time for property-carrying vehicles can not exceed 60hrs within 7 consecutive days.
Trigger Condition	Cumulative driving exceeds limit.
Device Functionality	Tracks driving hours.
Severity Level	Warning
Regulatory Impact	Driver compliance (FMCSA)
Applicable Device	eFuel

Activity ID: 046 – 70 Hour / 8 Day Limit

Activity Name	70 Hour / 8 Day Limit
Activity Category	Alert
Description	Driving limit as per FMCSA regulation, that driving time for property-carrying vehicles can not exceed 70hrs within 8 consecutive days.
Trigger Condition	Cumulative driving exceeds limit.
Device Functionality	Tracks driving hours.
Severity Level	Warning
Regulatory Impact	Driver compliance (FMCSA)
Applicable Device	eFuel

Addon data model

Power data model

Mandatory data for power status activity (activity 6/7):

Object	Description	Type
ext_power_voltage	External Power Voltage	Number
int_battery_voltage	Device Internal Battery Voltage	Number

Example:

```
{
    “ext_power_voltage”:”24.22”,
    “int_battery_voltage”:”3.89”
}
```

Trip data model

Mandatory data for deactivation activity (activity 27):

Object	Description	Type
distance_travelled	Distance travelled in km format	Number
trip_duration	Trip duration in minutes	Number
avgSpeed	Average speed (KM/h)	Number
maxSpeed	Max speed (KM/h)	Number

Example:

```
{
    “distance_travelled”:”505.2”,
    “trip_duration”:”400”,
    “avgSpeed”: “60”,
    “maxSpeed”: “85”
}
```

ESEAL Activation model

Mandatory data for deactivation activity (activity 16/17/18/19/25):

Object	Description	Type
seal_lock_left_status	The left side of seal lock status (Locked/Unlocked)	String
seal_lock_right_status	The right side of seal lock status (Locked/Unlocked)	String
seal_cable_status	Seal Cable status (Secured/Broken/Cut)	String
seal_lock_left_id	The detected tag ID for the left side lock header	String
seal_lock_right_id	The detected tag ID for the right side lock header	String

Example:

```
{
    “seal_lock_left_status”:”Locked”,
    “seal_lock_right_status”:”Locked”,
    “seal_cable_status”: “Secured”,
    “seal_lock_left_id”:”11223344”,
    “seal_lock_right_id”:”44332211”
}
```

Fuel Info data model

Object	Description	Type
validFlag	Data valid flag (0 for valid, other value to indicate non-valid fuel data)	Number
signalLevel	Received Signal Sensitivity of the fuel sensor (0-99)	Number
softStatus	Software status code (0 for normal)	Number
hardFault	Hardware fault code (0 for normal, see table 2 for details)	Number

fuelLevel	Fuel level (smoothed) in mm (Integer)	Number
rtFuelLevel	Real time fuel level in mm (Integer)	Number
tankTemp	Tank temperature in Celsius * (integer value with original temperaturex10, example: For 23.5 Celsius, 235 should be input in API)	Number
channel	Fuel tank compartment (integer value with default should be 1)	Number

Example:

```
{
  "validFlag": "0",
  "signalLevel": "75",
  "softStatus": "0",
  "hardFault": "0",
  "fuelLevel": "2100",
  "rtFuelLevel": "2134",
  "tankTemp": "312",
  "channel": "1"
}
```

Command Failure data model (For activity 28)

Object	Description	Type
txHash	The command hash send by system	String

Example:

```
{
  "txHash”: “XXXXXXXXXXXXXXXXXXXXXXXXXXXX”
}
```

Device Downlink commands with blockchain for enhanced security

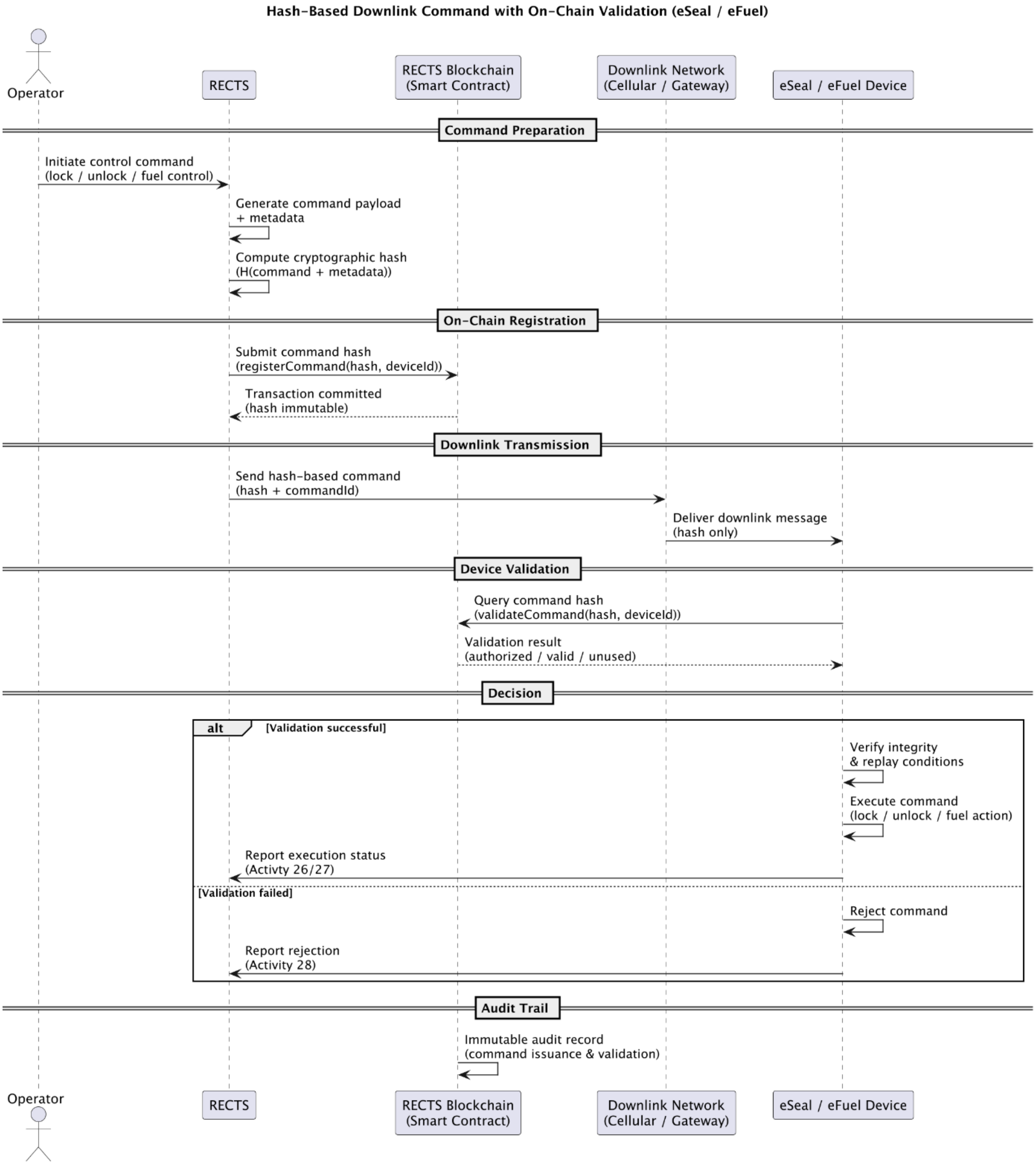
Overview

The system implements a secure command control mechanism for eSEAL and eFUEL devices using hash-based downlink commands combined with on-chain validation. Instead of transmitting full command payloads to devices, the backend generates a cryptographic hash representing the authorized command and registers it on a blockchain smart contract. The blockchain acts as a distributed and immutable source of truth for command authorization and device trust.

Only the compact hash value is transmitted to the device over the downlink channel, significantly reducing bandwidth usage and improving reliability in low-connectivity environments. Upon receiving the hash, the device (or an associated gateway) independently validates the command against the on-chain record, ensuring that the command is authorized, untampered, and has not been previously executed or revoked.

This approach enforces device-side trust validation, preventing unauthorized or forged commands even if backend systems or communication channels are compromised. The combination of off-chain command generation and on-chain authorization provides strong security guarantees, including integrity protection, replay attack prevention, decentralized trust, and full auditability. The architecture is well suited for regulated, multi-authority environments such as customs control, cross-border transit, and bonded logistics operations.

Downlink Flow Overview


Hash-Based Downlink Command with On-Chain Validation (eSeal / eFuel)
Operator
RECTS
RECTS Blockchain (Smart Contract)
Downlink Network (Cellular / Gateway)
eSeal / eFuel Device
Command Preparation
Initiate control command (lock / unlock / fuel control)
Generate command payload + metadata
Compute cryptographic hash (H(command + metadata))
On-Chain Registration
Submit command hash (registerCommand(hash, deviceId))
Transaction committed (hash immutable)
Downlink Transmission
Send hash-based command (hash + commandId)
Deliver downlink message (hash only)
Device Validation
Query command hash (validateCommand(hash, deviceId))
Validation result (authorized / valid / unused)
Decision
alt
[Validation successful]
Verify integrity & replay conditions
Execute command (lock / unlock / fuel action)
Report execution status (Activty 26/27)
[Validation failed]
Reject command
Report rejection (Activity 28)
Audit Trail
Immutable audit record (command issuance & validation)
Operator
RECTS
RECTS Blockchain (Smart Contract)
Downlink Network (Cellular / Gateway)
eSeal / eFuel Device

Step-by-Step Execution Flow (eSEAL / eFUEL)

Step 1 Command Creation (Off-Chain Backend)

- The backend system generates a control command (e.g. lock, unlock, fuel enable, fuel disable) together with contextual metadata such as device ID, timestamp, and command sequence.
- A cryptographic hash of the command payload and metadata is calculated.
- The full command payload remains off-chain and is not transmitted to the device.

Step 2 On-Chain Command Registration

- The generated command hash is submitted to the blockchain smart contract.
- The smart contract records the hash together with command metadata and authorization rules.
- Once committed, the hash becomes an immutable, authoritative reference for command validation.

Step 3 Downlink Transmission to Device

- The backend sends only the command hash (and minimal identifiers such as command ID) to the eSEAL / eFUEL device via the downlink channel.
- This minimizes data size and improves reliability in low-bandwidth or unstable networks.

Step 4 Device Receives Hash Command

- The device receives the hash-based downlink command.
- No sensitive command logic or business rules are exposed on the device at this stage.

Step 5 On-Chain Validation by Device (or Gateway)

- The device (or a trusted gateway acting on its behalf) queries the blockchain to verify:
- The hash exists on-chain
- The hash is associated with the correct device
- The command is authorized and not revoked
- The command has not been previously executed or expired

Step 6 Integrity and Replay Check

- The device ensures the received hash matches the on-chain record exactly.
- Sequence numbers, timestamps, or one-time-use flags are validated to prevent replay attacks.

Step 7 Command Authorization Decision

- If on-chain validation succeeds, the command is marked as authorized for execution.
- If validation fails, the command is rejected and logged without execution.

Step 8 Secure Command Execution

- The device executes the corresponding local action (e.g. seal lock/unlock, fuel control).
- Execution occurs only after successful on-chain validation.

Step 9 Execution Result Reporting

- The device reports execution status (success/failure) back to the backend.
- A confirmation hash or status update may also be recorded on-chain for audit purposes.

Step 10 Audit and Traceability

- The blockchain maintains an immutable record linking:
- Command issuance
- Authorization
- Validation
- Execution outcome
- This supports dispute resolution, regulatory audits, and cross-agency trust.

Example code of getting verification from blockchain

```
#!/usr/bin/env python3

import grpc
import json
from fabric_gateway import Gateway, Wallets

# ===========================
# CONFIGURATION
# ===========================
CHANNEL = "mychannel"
CHAINCODE = "fuel-config"
PEER_ENDPOINT = "<blockchainserverIP>:<port>"

TLS_CERT_PATH = "tls/ca.crt"
WALLET_PATH = "wallet"
IDENTITY_LABEL = "deviceClient"

DEVICE_ID = "EFUEL_001"
LOCAL_STATE_FILE = "fuel_state.json"

ALLOWED_FUEL_TYPES = {
    "WATER",
    "GASOLINE",
    "DIESEL",
    "KEROSENE",
    "ETHANOL"
}

# ===========================
# FABRIC CONNECTION
# ===========================
def get_contract():
    with open(TLS_CERT_PATH, "rb") as f:
        tls_cert = f.read()

    channel = grpc.secure_channel(
        PEER_ENDPOINT,
        grpc.ssl_channel_credentials(tls_cert)
    )

    wallet = Wallets.new_file_system_wallet(WALLET_PATH)
    identity = wallet.get(IDENTITY_LABEL)
    if not identity:
        raise Exception("Device identity not found in wallet")

    gateway = Gateway()
    gateway.connect(identity, channel, discovery=True)

    network = gateway.get_network(CHANNEL)
    return network.get_contract(CHAINCODE)

# ==========================
# LOCAL STATE (REPLAY PROTECTION)
# ==========================
def load_local_state():
    try:
        with open(LOCAL_STATE_FILE, "r") as f:
            return json.load(f)
    except:
        return {"version": 0, "fuel_type1": None}

def save_local_state(version, fuel_type):
    with open(LOCAL_STATE_FILE, "w") as f:
```

```
    json.dump({
      "version": version,
      "fuel_type1": fuel_type1
    }, f)

# =========================
# CHAIN QUERY
# =========================
def get_onchain_fuel_command(device_id):
  contract = get_contract()
  result = contract.evaluate_transaction(
    "GetFuelCommand",
    device_id
  )
  return json.loads(result)

# =========================
# SENSOR CONFIGURATION
# =========================
def apply_fuel_type_to_sensor(fuel_type):
  if fuel_type not in ALLOWED_FUEL_TYPES:
    raise Exception("INVALID_FUEL_TYPE")

  # === HARDWARE-SPECIFIC LOGIC GOES HERE ===
  # Example: select calibration table, density curve, etc.
  print(f"[DEVICE] Sensor configured for fuel type: {fuel_type}")

# =========================
# CORE ON-CHAIN VALIDATION
# =========================
def perform_onchain_fuel_type_check():
  print("[DEVICE] Checking on-chain fuel type configuration")
```

```
    local_state = load_local_state()
    local_version = int(local_state.get("version", 0))

    onchain = get_onchain_fuel_command(DEVICE_ID)

    onchain_version = int(onchain["version"])
    onchain_fuel = onchain["fuel_type1"]

    if onchain_fuel not in ALLOWED_FUEL_TYPES:
        raise Exception("ONCHAIN_FUEL_TYPE_NOT_ALLOWED")

    if onchain_version <= local_version:
        print(
            f"[DEVICE] No update needed "
            f"(local={local_version}, onchain={onchain_version})"
        )
        return

    print(
        f"[DEVICE] Fuel type change detected: "
        f"{local_state.get('fuel_type1')} → {onchain_fuel} "
        f"(v{onchain_version})"
    )

    apply_fuel_type_to_sensor(onchain_fuel)
    save_local_state(onchain_version, onchain_fuel)

    print("[DEVICE] Fuel type update applied successfully")

# =========================
# DOWNLINK HANDLER
# ==========================
def handle_downlink_command(downlink):
    # Downlink is only a trigger, never authoritative
    if downlink.get("command") == "SYNC_FUEL_CONFIG":
        perform_onchain_fuel_type_check()
    else:
        print("[DEVICE] Unknown downlink command ignored")

# ==========================
# MAIN ENTRY
# ==========================
if __name__ == "__main__":
    # Simulated downlink trigger
    downlink_message = {
        "command": "SYNC_FUEL_CONFIG"
    }

    try:
        handle_downlink_command(downlink_message)
    except Exception as e:
        print("[DEVICE] ERROR:", str(e))
```

Blockchain Access For Device Command Integration

Please engage with RECTS support group to get blockchain instance access

Smart Contract Data Model – eSeal

Attribute Name	Data Type	Description
device_id	String	Unique identifier of the eSeal device registered on the blockchain.
device_type	String	Device classification value identifying the device

		as an eSeal.
rects_comm_server	String	<domain>:<port> setting for RECTS comm server
registration_timestamp	Timestamp	Time at which the device was registered on-chain.
seal_status	Enum	Current seal state (e.g. Activated, Deactivated, Locked, Unlocked).
gps_reporting_interval	Integer	Regular reporting intervals for GPS tracking in seconds
trip_id	String	Identifier of the active trip associated with the seal, if applicable.
trip_route_points	String	Comma seperated <lat>:<lon>:<type> list for route detection. Possible type: plot/checkpoint/destination
trip_expected_time	String	The expected trip total time in minutes
state_version	Integer	Monotonically increasing version number representing the current seal state.
last_state_change_time	Timestamp	Time of the most recent seal state transition.
command_hash	Hash	Cryptographic hash representing an authorized control command.
command_type	Enum	Type of authorized command (e.g. Activate, Deactivate, Unlock).
command_status	Enum	Command lifecycle status (Authorized, Executed, Rejected, Expired).
command_valid_from	Timestamp	Start of command validity period.
command_valid_until	Timestamp	End of command validity period.
security_event_type	Enum	Reference to critical security events (e.g. Seal Cut, Illegal Activation).
security_event_time	Timestamp	Time at which the security event was recorded.

tx_id	String	Blockchain transaction identifier for traceability and audit.

Smart Contract Data Model – eFuel

eFuel Smart Contract Data Model (Multi-Compartment)

Attribute Name	Data Type	Description
device_id	String	Unique identifier of the eFuel master device.
device_type	String	Device classification identifying the device as eFuel.
rects_comm_server	String	<domain>:<port> setting for RECTS comm server
registration_timestamp	Timestamp	Time at which the eFuel device was registered on-chain.
gps_reporting_interval	Integer	Regular reporting intervals for GPS tracking in seconds
trip_id	String	Identifier of the active trip associated with the seal, if applicable.
trip_route_points	String	Comma seperated <lat>:<lon>:<type> list for route detection. Possible type: plot/checkpoint/destination
compartment_count	Integer	Number of active fuel compartments supported by the device (maximum 9).
compartments	Array	Collection of compartment configuration objects (see Table X-3).
command_hash	Hash	Cryptographic hash of an authorized configuration or control command.
command_category	Enum	Category of command (Configuration or Control).
command_status	Enum	Status of the command (Authorized, Executed, Rejected, Expired).

command_valid_from	Timestamp	Start time of command validity.
command_valid_until	Timestamp	End time of command validity.
integrity_event_type	Enum	Reference to integrity or security events related to sensors or casing.
integrity_event_time	Timestamp	Time at which the integrity event occurred.
tx_id	String	Blockchain transaction identifier for audit and traceability.

Fuel Compartment Configuration Object

Attribute Name	Data Type	Description
compartment_id	Integer	Logical compartment index (1–9).
sensor_id	String	Unique identifier of the fuel sensor attached to the compartment.
fuel_type	Enum	Authorized fuel type for the compartment (e.g. Diesel, Gasoline, Water).
config_version	Integer	Monotonically increasing configuration version for the compartment.
last_updated_at	Timestamp	Time when the compartment configuration was last updated.
updated_by	String	Identity of the authority that authorized the configuration change.
status	Enum	Compartment status (Active, Disabled, Fault).
tx_id	String	Blockchain transaction identifier for compartment configuration update.

Appendix II: Self-Financing Business Plan Template

Self-Financing Business Plan Template

1.0 Executive Summary

- **Mission & Vision:** Briefly define the goal (e.g., provide reliable, affordable tracking to small fleets).
- **Company Overview:** Name, legal structure (e.g., LLC), and location.
- **The Solution:** Describe your unique, self-financed service offering.
- **Financial Highlights:** Expected breakeven point and key, realistic milestones.

2.0 Company Description

- **Business Structure:** Owner-operated structure (limited partners/investors).
- **Mission & Philosophy:** Focus on high-quality service and organic growth.
- **Core Objectives:** Short-term (getting the first 5 clients) and long-term (market share).

3.0 Financial Plan (Self-Funded/Bootstrapping)

- **Startup Capitalization:** Detailed list of personal funds invested (hardware, software licenses, legal).
- **Break-Even Analysis:** Timeframe to reach positive cash flow (e.g., 6–12 months).