

DETAIL TECHNICAL SPECIFICATION

Supply, installation, and removal of intelligent driven smart container locks within the Transnet Operating Division (OD) of the Rail Infrastructure Manager (TRIM) nationally and internationally for a period of three (03) years.

1. SCOPE	2
2. BACKGROUND	2
3. STANDARDS AND APPLICABLE DOCUMENTS	2
4. DEFINITIONS AND ABBREVIATIONS	3
5. ENVIRONMENTAL CONDITIONS	6
6. QUALIFICATIONS	6
7. PERFORMANCE	6
8. REQUIREMENTS	7
9. TECHNICAL DOCUMENTATION	11
10. OPERATIONAL REQUIREMENTS	12
11. INTEGRATED SYSTEM REQUIREMENTS	15
12. SOFTWARE REQUIREMENTS	19
13. SAFETY	21
14. EQUIPMENT TESTING	21
15. QUALITY CONTROL	25
16. LEGAL OPERATIONAL	25
17. TENDERING PROCEDURE	26
18. INSPECTION AND QUALITY ASSURANCE	26
19. GUARANTEES AND DEFECTS	26
20. CONTRACT REQUIREMENTS	26
21. COMPLIANCE AND STANDARDS	31
22. COMPLIANCE TO STATUTES	33
23. DOCUMENTS PROPERTY OF THE CLIENT	34

Respondent's Signature

Date & Company Stamp

1. SCOPE

Given the high level of losses associated with theft of containers and cargo, TFR, intends to implement an intelligent driven smart container locking system and services contract to reduce theft of containers and cargo in transit, Marshalling Yards, as well as Container Terminals.

The purpose of this document is to explicitly outline the functional requirements and expectations for the supply, installation, and removal of intelligent driven smart container, sugar wagon, and beer wagon locks, providing a comprehensive understanding of the security needs and responsibilities required to ensure the effective protection of cargo.

2. BACKGROUND

Transnet Freight Rail (TFR) is in the business of moving containerised and bulk commodities by rail. Due to the current socio-economic conditions in the country, the commodities are targeted on a regular basis by common criminals and organised crime syndicates.

Cargo theft is a significant challenge and a common occurrence for TFR, resulting in financial losses and operational disruptions. To combat this, TFR introduced a container locking system to protect commodities in transit and Container Terminal Depots.

The existing container locking contract has provided effective security measures for TFR's cargo. However, with its impending conclusion, it is crucial to initiate the procurement process for a new service to avoid any lapse in security. The new service must meet or exceed the current security standards to protect cargo.

3. STANDARDS AND APPLICABLE DOCUMENTS

Unless otherwise specified all materials and equipment supplied shall comply with the applicable and latest editions of SANS, BS, IEC or Transnet Freight Rail's publication where applicable.

3.1 Transnet Documents

- 3.1.1. CSE 1154-001 Cat. E48: Environmental Specification for Transnet Railway Signalling Systems.
- 3.1.2. CSE_1133_052_Cat.98: Corrosion Resistant.
- 3.1.3. CEE-0188.89: Photo electric control unit.

Respondent's Signature

Date & Company Stamp

- 3.1.4. CEE- 0224: Drawing, Catalogues, instruction manual and spare lists for electrical equipment supplied under contract.
- 3.1.5. E4E: Safety Arrangement and Procedural Compliance with the Occupational Health and Safety Act (Act 85 of 1993) and Applicable Regulations.
- 3.1.6. BBD- 8210: E7/1 – Specification for General Work and Works On, Over, Under or Adjacent to Railway Lines and Near High Voltage Equipment.

3.2. South African National Standard Documents

- 3.2.1. SANS 10238, SABS 0238, Welding and thermal cutting processes – Health and safety
- 3.2.2. EN1300 – Secure storage units – Classification for high security locks according to their resistance to unauthorized opening.
- 3.2.3. SANS 279 – Paints and varnishes – Scratch test.
- 3.2.4. SANS 2409 – Paints and varnishes – Crosscut test.
- 3.2.5. SANS 10238 – Welding and thermal cutting processes – Health and safety.
- 3.2.6. SANS 15026:1998- Information Technology - System and Software Integrity Levels.
- 3.2.7. SANS 15816:2006 - Security techniques — Security information objects for access control.

3.3. International Organization for Standardization

- 3.3.1. IEC 9126 - Software engineering — Product quality

3.4. Statutory Requirements

- 3.4.1. OHS Act 85 of 1993- Occupational Health and Safety Act.

4. DEFINITIONS AND ABBREVIATIONS

4.1. Definitions

Unless the context indicates otherwise, the words and expressions set out below shall bear the following meanings and cognate expressions shall bear corresponding meanings:

- 4.1.1. Whenever "Transnet" is used in the generic specifications, it should be read as "the Employer", and wherever "engineer" or similar terminology is used, it should be read as "the Engineering/Project Manager".
- 4.1.2. The Employer for this Contract is Transnet, SOC Ltd, trading as Transnet Freight Rail. The requirements are based on the Transnet Freight Rail specifications.

Respondent's Signature

Date & Company Stamp

- 4.1.3. The information and or requirements as stated in Transnet Freight Rail's specifications shall be considered as the minimum requirements for equipment to be offered.
- 4.1.4. Whenever "Technical Officer or Site Agent" is used in the specification it refers to Transnet Freight Rail's Contract Supervisor or his appointed representative.
- 4.1.5. Geo-fence locking capabilities – Geo-fencing is a location-based service in which an application or other software uses GPS, RFID, Wi-Fi or cellular data to trigger a pre-programmed action when a mobile device or RFID tag enters or exits a virtual boundary set up around a geographical location, known as a geofence. The smart lock geofencing capabilities must raise alerts when locks are removed from designated areas.
- 4.1.6. Tamper proof - is resistance to tampering (intentional malfunction or sabotage) by either the normal users of a product, package, or system or others with physical access to it. Anti-tamper devices have one or more components: tamper resistance, tamper detection, tamper response, and tamper evidence.
- 4.1.7. Wireless - wireless is the term used to describe any network where there is no physical wired connection between sender and receiver, but rather the network is connected by radio waves, microwaves, etc. to maintain communications.
- 4.1.8. Manufacturer - person or company that makes goods for sale.
- 4.1.9. Supplier - person or organization that provides something needed such as a product or service.
- 4.1.10. Contractor - a person or firm that undertakes a contract to provide materials or labour to perform a service or do a job.
- 4.1.11. Qualified technician – Transnet personnel officially recognized as being trained, skilled, and certified to perform a particular job, with a practical understanding of the relevant engineering concepts.
- 4.1.12. Standard working procedure - is a set of step-by-step instructions compiled by TFR to help workers carry out complex routine operations.
- 4.1.13. Ergonomics - an applied science concerned with designing and arranging things people use so that the people and things interact most efficiently and safely.
- 4.1.14. Keyless - keyless is an entry system that controls operation of lock without using a traditional mechanical key.
- 4.1.15. Smart key - is a key with digital or information features that can facilitate more functionality than just unlocking a physical or digital lock system.
- 4.1.16. Lock - a mechanism for keeping a door, window, lid, or container fastened, which will deny entry to unauthorized people.

Respondent's Signature

Date & Company Stamp

- 4.1.17. Digital key - key employed to ensure that data exchanged during an electronic transaction remains unchanged and cannot be interfered with by any third party.
- 4.1.18. Fail safe locking protocol - in engineering, a fail-safe is a design feature or practice that in the event of a specific type of failure, the system inherently responds in a way that will cause no or minimal harm to other equipment, to the environment or to people.
- 4.1.19. Real time – within 5 minutes or less, after the occurrence of an incident.

4.2. Abbreviations

- 4.2.1. ISO - International Organization for Standardization
- 4.2.2. TFR - Transnet Freight Rail
- 4.2.3. SABS - South African Bureau of Standards
- 4.2.4. SANS - South African National Standards
- 4.2.5. SANAS - South African National Accreditation System
- 4.2.6. SLA - Service Level Agreement
- 4.2.7. ICASA - Independent Communications Authority of South Africa
- 4.2.8. GPS - Global Positioning System
- 4.2.9. GSM - Global System for Mobile Communications
- 4.2.10. GPRS - General Packet Radio Service
- 4.2.11. WAN - Wide Area Network
- 4.2.12. APN - Access Point Name
- 4.2.13. UDP - User Datagram Protocol
- 4.2.14. TCP/IP - Transmission Control Protocol / Internet Protocol
- 4.2.15. OEM - Original Equipment Manufacturer
- 4.2.16. SMS - Short Message Service
- 4.2.17. GIS - Geographic Information System
- 4.2.18. SWP- Standard Working Procedure
- 4.2.19. SOP - Standard Operating Procedure
- 4.2.20. IP - Ingress Protection
- 4.2.21. IEC - International Electro technical Commission
- 4.2.22. ETA - Expected Time of Arrival

Respondent's Signature

Date & Company Stamp

5. ENVIROMNETAL CONDITIONS

- 5.1 The intelligent driven smart rail container and wagon locks shall be used across the entire country of South Africa, consequently the locks will need to operate in the diverse weather conditions found in South Africa. The locks will operate under the following weather conditions.
- 5.1.1 Ambient air temperature of -10°C up to 60°C
 - 5.1.2 Atmospheric pressure of 50kPa up to 102 kPa
 - 5.1.3 Altitude of 0m up to 1800m above sea level
 - 5.1.4 Relative humidity of 10% up to 90% percent
 - 5.1.5 Wind speed of 0 km/h up to 60km/h
 - 5.1.6 Precipitation of 20mm a day
 - 5.1.7 Solar radiation of 4 kWh up to 6 kWh (Daily totals)
 - 5.1.8 Airborne salinity of $300 < S$ (Deposition rate of NaCl, mg/m² per day)
 - 5.1.9 Pollution Heavily salt laden or polluted with smoke from industrial sources.
- 5.2 The expectation is the rail container and wagon locks will be fully functional under the adverse weather conditions stated above.

6. QUALIFICATIONS

- 6.1 The design of the rail container and wagons locks are to be that of the manufacturer but must be of robust construction in to meet sustained heavy duty demands, yet they must be safe to use.
- 6.2 The rail container and wagon locks will be acceptable in standard factory production finish and colour.
- 6.3 The supplier shall provide training for relevant personnel on how to use the lock and entire system.
- 6.4 The lock and system shall be availed by the supplier for testing purpose.

7. PERFORMANCE

- 7.1 The rail container and wagon locks are to be easily and economically maintained/repared with standard workshop tools and equipment when necessary.

8. REQUIREMENTS

- 8.1 The actual design of the intelligent driven lock for rail containers and wagons shall meet the requirements below.

Respondent's Signature

Date & Company Stamp

- 8.1.1 The intelligent driven smart locks should be designed to address the challenges of managing access to rail container and wagons.
- 8.1.2 The solution provided should ensure transparency and protect TFR's assets from unauthorized users. Operations should be logged to ensure traceability.
- 8.1.3 The solution should be secure, scalable, and easy to retrofit to existing railway container, sugar wagon, and beer wagon doors and frames.
- 8.1.4 The general railway container and wagon lock shall be constructed and assembled such that any component can be repaired or replaced by properly qualified technicians without undue difficulty.
- 8.1.5 The manufacturer of the lock shall ensure that spare components for the lock will be available for at least five years post manufacturing of the lock.
- 8.1.6 The railway container and wagon lock shall be manufactured in a way that it can be easily locked and unlocked.
- 8.1.7 The railway contain and wagon lock shall be constructed of materials that are acceptably resistant to corrosion and wear.
- 8.1.8 The Contractor must provide the suppliers or manufactures of the lock material and equipment with a copy of the equipment specification to ensure compliance.
- 8.1.9 The Contractor shall supply all railway container and wagon locks which shall be according to Transnet Freight Rail specifications and SABS.
- 8.1.10 The contractor shall execute the works in accordance with Transnet specification **E7/1** and **E4E**.
- 8.1.11 The contractor shall commence work within period specified on a schedule plan and completion period shall be indicated.
- 8.1.12 Clear and concise relevant documentation such as the user manual, installation manual and datasheets shall be supplied with the bid.
- 8.1.13 The locking mechanism's embedded tracking equipment shall adhere to all ICASA regulations.

8.2 Technical Requirements

- 8.2.1 The intelligent driven smart lock monitoring and management platform should be developed to work seamlessly on desktop, Android, and iOS.
- 8.2.1 The solution should allow TFR's technical staff to manage secure digital tokens, to track lock operations directly between authenticated mobile phones and the smart locks, and to

Respondent's Signature

Date & Company Stamp

customize levels of control. The platform should provide real-time data and it should be easy to use for the end users.

8.3 Tracking with full audit capabilities

- 8.3.1 Indicate or track who has accessed TFR's assets/sites at a glance and the amount of time spent on site.
- 8.3.2 Connected GPS should display all the locations of the locks and operations.

8.4 Smart lock management and control system

- 8.4.1 Highly secure system control who gets authorization to access sites or properties.
- 8.4.2 Full audit trail which should allow visibility on access records as well as time spent on site.

8.5 Control room

- 8.5.1 The contractor shall setup and install the intelligent driven smart lock application monitoring and management system in TFR's Nerve Centers nationally to monitor all alarms and notifications coming from the smart locks.
- 8.5.2 The contractor shall notify Transnet stakeholders of alarms and notifications in real time.
- 8.5.3 The contractor shall notify a minimum of 10 Transnet stakeholders, number of Transnet stakeholders be adjusted as per needs of the organization.
- 8.5.4 The control room shall be operational on a twenty-four hour, seven days a week basis.

8.6 Keyless Operation

- 8.6.1. Operation should require no physical keys and done via Bluetooth or RFID, or any other battery powered remote control communication medium. The wireless key shall be traceable through GPS and linked to a user interface to track and trace the operational key.
- 8.6.2. Digital keys provide heightened levels of security for sites and properties as unauthorized distribution or duplication of physical keys are eliminated.
- 8.6.3. Digital keys shall be designed such that it is applicable to general railway container and wagon locks.
- 8.6.3 The smart locks must be designed to alleviate theft of containers and theft out of containers.
- 8.6.4 The smart lock system must be web based and allow the mobile device and computer to access the locks and enable locking and unlocking of the locks from a TFR Control Room. The methodology of remote unlocking and locking must be secure.

Respondent's Signature

Date & Company Stamp

- 8.6.5 The smart lock shall have special mechanisms designed to lock (install) and unlock (remove) these locks (such as a key, electronic key card, fingerprint, Radio Frequency Identification (RFID) card, security token etc.). The lock shall have an override key to lock and unlock the locks in the event of system malfunctions. The bidding company must ensure adequate security and management of the override key.

8.7 Material properties

- 8.7.1 Material used to manufacture the locking device should not be from copper or other high value material due to its high street value for criminals.
- 8.7.2 The lock barrier materials must be corrosion resistant.
- 8.7.3 The smart locks shall be manufactured from hardened steel or any other element or material that will be able to withstand the technical tests as provided for by TFR. To ensure compatibility, the smart container locks proposed shall accommodate various container including but not limited to the types on Table 1.

Containers	Sugar wagons	Beer wagons	Fuel tankers	On request
6-meter 12-meter - All configurations	FCJ	FSLJ	- JET 343 - Petrol - Diesel 877	- SARU containers - Reefer container - Tanker Wagons

Table 1: Types of containers.

- 8.7.4 The lock shall be capable of passing tests given in Section 14.

8.8 Ingress Protection (IP)

- 8.8.1 The IP Code (or International Protection Rating, sometimes also interpreted as Ingress Protection Rating*) consists of the letters IP followed by two digits and an optional letter. As defined in international standard IEC 60529, it classifies the degrees of protection provided against the intrusion of solid objects (including body parts like hands and fingers), dust, accidental contact, and water in electrical enclosures. The standard aims to provide users more detailed information than vague marketing terms such as waterproof.
- 8.8.2 The railway container and wagon lock will require a minimum IP66 rating. The lock offered is subject to testing at the lab. Relevant certificates, reports shall be submitted from independent, accredited laboratory or testing facility.

Respondent's Signature

Date & Company Stamp

8.8.3 Table 2 is an easy-to-follow reference on the IP ratings. The bidding company must submit the technical specification of the lock with the bid.

IP NUMBER	FIRST DIGIT - SOLIDS	SECOND DIGIT - LIQUIDS
IP65	Protected from total dust ingress.	Protected from low pressure water jets from any direction.
IP66	Protected from total dust ingress.	Protected from high pressure water jets from any direction.
IP67	Protected from total dust ingress.	Protected from immersion between 15 centimeters and 1 meter in depth.
IP68	Protected from total dust ingress.	Protected from long term immersion up to a specified pressure.
IP69K	Protected from total dust ingress.	Protected from steam-jet cleaning.

Table 2: Ingress Protection table

8.9 Weight

8.9.1 Based on operational standard working procedure and ergonomics, the locking device shall be restricted to a maximum weight of 5 kilograms.

8.10 Dimensions

8.10.1 The dimensions of the locking device will be limited to the railway container, sugar wagon, and beer wagon doors.

8.11 Appearance

8.11.1 Only the lock status shall be visible on the lock. However, efforts should be made to not make it visible to the public. No other monitoring signals or indicators such as signal strength, battery life, etc. shall be visible on the lock.

Respondent's Signature

Date & Company Stamp

8.12 Finish

- 8.12.1 All machined parts of a lock shall have a smooth finish and shall be free from ragged edges and tool marks.
- 8.12.2 When not made of a metal that is inherently corrosion resistant, the door and its locks and bolt work shall be so protected as to resist the corrosive influence on which they are expected to be subjected in normal service.

8.13 Life cycle

- 8.13.1 One unit to last a minimum of 5 years under normal operating conditions.

8.14 Maintenance

- 8.14.1 Minimum of a 6-month maintenance interval or on demand maintenance request in special conditions. The maintenance of the smart locks must be done by the contractor for the duration of the contract.

9. TECHNICAL DOCUMENTATION

- 9.1 Technical documentation of the intelligent driven smart lock shall include the following information provided with the bid submission:
- 9.1.1 The date of issue and the name of the manufacturer shall be on each page.
 - 9.1.2 Statement of the type of product: general container lock.
 - 9.1.3 Drawings of the lock shall show the following:
 - 9.1.3.1 Mass, outside and inside dimensions, and the manufacturing tolerances.
 - 9.1.3.2 Horizontal and vertical cross sections.
 - 9.1.3.3 Quantity, layout and features of locks, bolt work and relocking devices.
 - 9.1.3.4 Quantity, pitch and position of bolts, their dimensions (for example, cross section), throw and engagements and their type (for example, moving or fixed).
 - 9.1.3.5 Location and design of any local areas of special protection materials.
 - 9.1.3.6 Marking, position and dimensions of any holes which pass through the protection material with a detailed representation of specially protected areas.
- 9.2 List of all the locks which may be fitted, giving the manufacturer and model number.
- 9.3 Statements of the nature and position of any cables or facilities (or all of these) for penetration.

Respondent's Signature

Date & Company Stamp

- 9.4 Detection systems, for the mounting of electro-mechanical securing devices, alarm devices or other.
- 9.5 The method by which the lock is anchored to the door frame or other surface.

10. OPERATIONAL REQUIREMENTS

- 10.1.1 Digital keyless lock must be durable and strong
- 10.1.2 Operating temperature should be -10°C up to 60°C
- 10.1.3 It should be weather resistant – at least IP66 rated
- 10.1.4 It should generate critical reports for data analysis
- 10.1.5 The lock shall be compatible with:
 - 10.1.5.1 Either Bluetooth, RFID, or any other wireless communication medium
 - 10.1.5.2 Any iOS system
 - 10.1.5.3 Any Android system
 - 10.1.5.4 Windows OS

10.2 True Keyless Solution

- 10.2.1 The lock should only allow authorized personnel to have a virtual key of unlocking/locking the intelligent driven smart lock. For security, each virtual key should be protected by a stipulated time limit and only pre-approved users should be able to request for access. No duplications shall be allowed.

10.3 Grouping users by infrastructure depots, regions, use cases or tasks

- 10.3.1 Allow user's identity and information to be provided by Transnet and preset on the system. Only authorized personnel should have access to the smart locks.

10.4 Wireless communication medium virtual keys to operate smart locks

- 10.4.1 Admin/Skeleton/Master virtual keys
- 10.4.2 Repeating tasks/schedule virtual keys
- 10.4.3 One-time access virtual keys
- 10.4.4 Allow authorized users to request for virtual keys
- 10.4.5 Track and trace functionality of each wireless key.
- 10.4.6 Remote key reset or cancellation by senior TFR authorised personnel.

Respondent's Signature

Date & Company Stamp

10.5 Offline mode

10.5.1 Authorized personnel should be granted access on virtual keys to log into the application and operate the virtual key offline in case there is no network or Wi-Fi connection. To ensure site security, Offline mode should only be operated within a stipulated time limit from the time the user accepts the job.

10.6 Classify/Block specific periods of time for scheduling tasks in a restricted zone

10.6.1 Tasks should be scheduled as a basic for any asset access control system. The system should provide ability to schedule periodic tasks for up to 20 sets of specific dates in a specific period.

10.7 Consolidate management and access control system into one platform

10.7.1 The access control methods for the locks shall be dictated by Transnet as per the business requirements. Access control for all the contractors, in-house engineers, etc. should be managed on one platform to minimize the amount of work for any admin/managers-in-charge.

10.8 Access permission verification process

10.8.1 Enhance security by assigning the right person in charge for each region, contracting company or infrastructure depot to be responsible of overseeing, granting and approving accesses to operate the smart locks.

10.9 Regional or global operational trackers

10.9.1 System should have a global set-up of all our railway container and wagon locks using the same software for separate entities in different business units or regions.

10.10 Enhance search-ability power

10.10.1 The system should consist of a search function, which will be a powerful tool to find accountable personnel in case of emergency.

10.11 Data Analysis

10.11.1 System should be able to generate task performance by tracking and analyzing every smart lock operation. This will enable easy benchmarking of productivity across all individuals or contractors working on site.

Respondent's Signature

Date & Company Stamp

10.12 Real-time Auditing Tool

10.12.1 Software should allow asset auditors to audit access security process and find information quickly via the platform.

10.13 Picture verifications for site security

10.13.1 All users should be required to take a picture of the site after operation on any railway container and wagon lock to prove attendance and job done.

10.14 Power supply

- 10.4.1 The system should have its own power supply with at least six months maintenance period (i.e. six months to replace the battery/power source). The system should be designed in such a way that even if the power is lost from the main source, it should have a back-up/alternative to allow for the lock to be manually operated. Free-standing units shall possess battery units to ensure operation for at least 3 years. The wireless, battery powered keys shall utilize rechargeable batteries and be integrated to a charging station for extended use. The charging station shall be provided by the contractor. The battery units incorporated in the locks and keys shall be standard size and rating such that it is readily available in the South African market.
- 10.4.2 The smart lock system must be powered up by rechargeable batteries which have a 3-year life span or more. The bidding company must submit the technical specifications of the battery with the bid.
- 10.4.3 The system must have a feature to alert the Control Centre in the event of battery discharge and shall not lose its optimal functionality when the battery is discharged.

11. INTEGRATED SYSTEM REQUIREMENTS

- 11.1.1 Remote locking is an essential requirement to secure and facilitate the protection of Transnet Freight Rail's assets, thus each lock shall be developed such that it enables remote triggering through a digital key.
- 11.1.2 Upon the unlocking of an asset, employee validation shall be done through the request of employee credentials and the validation thereof through a secure and linked database. Validation shall be done through engagement with either a control centre or through secure password validation or any secure means.
- 11.1.3 A successful validation shall then permit the user to operate the relevant asset lock, using the wireless battery powered key, and log the details of the individual who accessed the asset, the time, date and credentials of the individual who authorized the unlocking event.

Respondent's Signature

Date & Company Stamp

- 11.1.4 The developed system shall store these details in the database of the system which can be accessed only by the administrator or relevant personnel in the control centre or Transnet employees. The system and the contractor shall generate automated reports periodically being either daily, weekly, monthly, yearly or upon request by Transnet based on the timeframe requirements.
- 11.1.5 The system shall be usable with low physical and cognitive effort by a widespread population and shall cater to individuals who are physically incapacitated.
- 11.1.6 The system shall be developed such that unique digital keys are implemented to accurately distinguish individual characteristics. The implemented system shall also be robust such that weather or any adverse environmental conditions do not affect the operation of the locking system. This addresses the operation Bluetooth, RFID or any other digital medium for asset unlocking.
- 11.1.7 The system should be able to collect the characteristics easily from the subjects and the characteristics should be sufficiently distinct and repeatable to achieve successful recognition of the subject as per SANS 24745:2013.
- 11.1.8 The system shall be spoof resistant, which indicates the difficulty to which it is able to replicate the individual digital key characteristics, being either password or control centre based to circumvent the locking system.
- 11.1.9 The system shall be able to frequently update the stored profile for each individual and build an employee profile to ensure that false or unauthorized access is mitigated.
- 11.1.10 The operational time limits for the digital key validation shall comply with the time requirements set as per SANS 2220-2-5 clause 4.3.1. The digital key shall possess an embedded GPS unit which allows the key to be tracked and monitors the frequency and usage (date and time) of the key.

11.2 Locking/Unlocking

- 11.2.1 To lock a digital keyless lock means to use a device or mechanism for securing the railway infrastructure doors or switch structure in position through a mechanism operated by a key, dial, electronics etc. The locking features required for the locking mechanism are as follows:
- 11.2.1.1 Remote and wireless locking.
- 11.2.1.2 Keyless system – a physical key must not be used to open/close the asset.

Respondent's Signature

Date & Company Stamp

- 11.2.1.3 Digital key or electronic key – key employed to ensure that data exchanged during an electronic transaction remains unchanged and cannot be interfered with by any third party.
- 11.2.1.4 The digital key should be used in case of any emergency (e.g. emergency fault which impacts trains movement)
- 11.2.1.5 Geo fence locking capabilities – Geo-fencing is a location-based service in which an app or other software uses GPS, RFID, Wi-Fi or cellular data to trigger a pre-programmed action when a mobile device or RFID tag enters or exits a virtual boundary set up around a geographical location, known as a geo-fence.
- 11.2.1.6 Fail safe locking protocol.
- 11.2.1.7 Lock must not detach or fall off from railway asset door or switch structure until physically removed.
- 11.2.1.8 Relevant notifications should be sent from the lock to a mobile and computer application to indicate the lock status.
- 11.2.1.9 The locking mechanism shall encompass user-friendly attributes.
- 11.2.1.10 Operational time for either locking or unlocking shall not take more than 2 minutes.
- 11.2.1.11 The maximum number of people allowed to operate the locking mechanism is one person.

11.3 Tamper detection

- 11.3.1 The smart container locks shall have tamper detection capability to prevent or minimize the unlawful removal from the containers. These locks will be fitted on sensitive cargo. Therefore, the smart locks shall have capabilities to set the detection rate in various environments and weather conditions. The smart container lock shall facilitate awareness of tampering with the locking devices in real time at the TFR Security Control Room.
- 11.3.2 The lock must have the ability to detect and respond with an appropriate alarm to the following intrusion activities:
 - 11.3.2.1 Bending of railway container and wagon doors or switch structure frame.
 - 11.3.2.2 Striking of a container and wagon doors or switch structure frame.
 - 11.3.2.3 Cutting of a railway container and wagon doors or switch structure frame.
 - 11.3.2.4 Pulling of railway container and wagon doors or switch structure frame.
 - 11.3.2.5 Departure of a lock from a geo-fenced area.
 - 11.3.2.6 Magnetic tampering.

Respondent's Signature

Date & Company Stamp

11.3.2.7 Signal jamming.

11.4 Wireless remote monitoring system

11.4.1 The wireless remote monitoring system shall have the following capabilities:

- 11.4.1.1 Real time monitoring with a maximum of a 10 minute- refresh rate.
- 11.4.1.2 Remote, wireless, and centralized monitoring.
- 11.4.1.3 Web and App/ cell phone access.
- 11.4.1.4 Compatible with Windows, Android and IOS system.
- 11.4.1.5 GPS location of lock and battery powered wireless key.
- 11.4.1.6 All units must be visible on one monitoring unit.
- 11.4.1.7 Trigger alarms for all sensors in both an audio and visual format.
- 11.4.1.8 Low battery warnings.
- 11.4.1.9 Record keeping of operators who conducted the lock and unlocking of the locking units with date and time stamps.
- 11.4.1.10 The platform shall be fully customizable to suit the needs of the client.
- 11.4.1.11 The minimum parameters that must be able to be accessed on the remote monitoring user interface are as follows:
 - 11.4.1.12 Equipment/asset number
 - 11.4.1.13 Power/battery life.
 - 11.4.1.14 Status of all sensors.
 - 11.4.1.15 GPS location.
 - 11.4.1.16 Lock/unlock position
 - 11.4.1.17 Nearest depot.
 - 11.4.1.18 Number of days until the next maintenance of lock
 - 11.4.1.19 Signal strength.
 - 11.4.1.20 Date and Time stamping
 - 11.4.1.21 Full name and SAP number/Employee number of person who locked and unlocked a digital lock.

11.5 Mobile phone application and web interface

- 11.5.1 Includes Global Positioning System (GPS) and Global System for Mobile communication (GSM) or any other communication medium modules built to send GPS data of lock to main server.
- 11.5.2 The embedded software should analyse the GPS data and provide a navigation display.

Respondent's Signature

Date & Company Stamp

- 11.5.3 The data from the lock are encrypted using AES algorithm or any other industry accepted secured algorithm before sending it to the web server.
- 11.5.4 The programming language used to develop the application shall be such that the application can be installed and can run on different models of mobile phones without any major changes on the application.
- 11.5.5 Data of the GPS co-ordinates accessed through every mobile phone device must be stored in the Transnet server.
- 11.5.6 The mobile application should be able to give exact location in terms of latitude and longitude coordinates accurate to within a range of 10 meters to approximately 1 meter and the precise time accurate to within a range of 60 ns to approximately 4 ns.
- 11.5.7 The authorized user needs to enter username and password to provide authentication with the server or mobile application.
- 11.5.8 The position pins should be indicated with a different colour for any digital lock locked, unlocked, and requiring maintenance.

12. SOFTWARE REQUIREMENTS

- 12.1.1 The lock shall be fully integrated with a platform and unlimited access shall be granted. The platform shall be accessible from either Internet Explorer, Microsoft Edge or Google Chrome. The platform shall also be configured such that no plug-ins are required to access the user interface. Mobile device-based platforms shall be configured such that it is operable on both iOS and Android devices.
- 12.1.2 The platform must be updated based on data received from devices in near real-time as per any tampering or Geo-Fence boundary exceedance. One shall also be able to use the platform to track and trace the locking devices and the battery powered wireless keys.
- 12.1.3 The platform shall be developed such that it is compatible with most recent Microsoft Windows versions, and compatible with both 32 bit and 64bit processors.
- 12.1.4 The platform must be able to display all devices on one page or customized to show selected devices. The conditions for displaying the various devices shall allow for topographical, satellite, and map view, as well as a tabulated list.
- 12.1.5 The platform must give full administration rights to the owner and Transnet at no additional cost.
- 12.1.6 The lock platform must have customizable alerts in the form of both visual and audible notifications.

Respondent's Signature

Date & Company Stamp

- 12.1.7 Visual notifications shall take the form of colour identifications and pop-up messages. Sound notifications shall take the form of customizable tone settings.
- 12.1.8 In addition, access shall be granted to the raw data received from the devices by means of the platform.
- 12.1.9 The data received from the devices shall be in such a format that it can be integrated into an existing Transnet monitoring system.
- 12.1.10 The devices shall be independently identifiable from the platform, and one should be able to monitor the locked or unlocked status of a specific lock. The platform shall also allow the owner and Transnet to rename the devices accordingly and create a customizable Geo-Fence for each device.
- 12.1.11 The user interface shall require secure Transnet login credentials to access the platform and monitor/adjust the data and devices.
- 12.1.12 The user interface shall be developed such different work grades are able to monitor different items based on the level of authority or clearance. The platform shall also generate reports based on employee access and modifications on-demand being either daily, weekly, monthly, or yearly.
- 12.1.13 All reports shall be developed such that it can be downloaded to a personal computer or mobile device.
- 12.1.14 The user interface shall enable employees employed in the relevant control centres to remotely unlock the relevant assets, from the control centre, based on the business need.
- 12.1.15 The user interface shall be developed such that all the functionality, reliability, usability, efficiency, maintainability, and portability attributes comply with IEC 9126.

12.2 Security, encryption, and data integrity requirements

- 12.2.1 Data transmitted to the platform shall employ the relevant Advanced Encryption Standards (AES) in all encryption and decryption techniques to prohibit signal hacking, eavesdropping and the loss of data integrity.
- 12.2.2 False rejection rate of authorized users shall be not more than one in twenty.
- 12.2.3 The software integrity requirements for the user interface shall be such that it adheres to SANS 15026:1998.
- 12.2.4 The security protocols shall be implemented such that it complies with SANS 15816:2006. All data must be encrypted and treated as confidential.

Respondent's Signature

Date & Company Stamp

12.3 Database requirements

- 12.3.1 The database developed for the locking system shall be compliant with the relevant and most recent Transnet ICT standards.
- 12.3.2 Full administration rights to the database shall be given to Transnet at no additional cost and maintenance work of the database shall be carried out by the contractor for the contract duration.
- 12.3.3 The database shall be developed such that it can be integrated or merged to existing Transnet databases.
- 12.3.4 Adequate storage and records shall be allocated within the databases to enable the development of an employee profile to aid in fault or user credential management. This includes generating new digital keys and detailing the history of previous digital keys allocated to an employee.
- 12.3.5 Security layers shall be implemented between the database and the user interface as per SANS 15816:2006.

13. SAFETY

- 13.1 The contractor or his sub-contractor shall be required to work on site in accordance with Transnet Freight Rail's safety specification E4E of April 1997 and the occupational health and safety act 85 of 1993.
- 13.2 The contractor shall be required to work under direct supervision of Transnet Freight Rail's depot personnel on site and shall work only in the area which shall be demarcated by suitable barriers.

14. EQUIPMENT TESTING

- 14.1 The smart locking devices are subjected to testing which these tests are conducted using the set-out test experiments. The tests may be uniquely designed for specific testing purpose, but also standard testing is required which is included on some of the standards in Section 3 of this document.

14.2 Electronic and Electrical Tests**14.2.1 Testing of sensors and anti-tempering capabilities**

TFR reserves the right to develop a bespoke test procedure to test and validate the performance of the sensors and anti-tempering capabilities of the general railway container, sugar, and beer wagon lock. This test procedure will be based on the specifications of TFR.

Respondent's Signature

Date & Company Stamp

14.2.2 Signal jamming

Transnet Freight Rail reserves the right to develop a signal jamming test procedure to test and validate the performance of the sensors and anti-tempering capabilities of the general railway container and wagon lock.

14.2.3 Power supply test

Transnet Freight Rail reserves the right to develop a power supply test procedure to test and validate the performance of the sensors and anti-tempering capabilities of the general railway container and wagon lock.

14.3 MECHANICAL TESTS

TFR requires to perform destructive testing on a sample lock to understand a specimen's performance and material behaviour, this procedure is carried out to test specimen's failure. Destructive testing methods will be used for failure investigation and form part of the engineering assessment. Destructive testing procedures can either follow specific standards or can be tailored to reproduce set service conditions. Due to Transnet's unique railway environment, a bespoke test procedure has been developed and will be used to determine if the locking solution is railway worthy. **The test procedure is provided in Appendix A.** The types of destructive testing are as follows:

14.3.1 Aggressive environment testing

This includes fracture and fatigue testing in sour (H₂S), sweet (CO₂) and other corrosive environments, at a range of temperatures and pressures. This test allow industry to assess the impact of these conditions on materials and performance.

14.3.2 Corrosion testing

This covers non-toxic, small-scale, aqueous corrosion testing in a variety of different environments including fresh and sea water.

14.3.3 Fracture and mechanical testing

This includes different types of destructive testing methods such as tension tests, bend tests, Charpy impact tests, Pellini drop weight testing, peel tests, crush testing, pressure, and

fracture testing. As well as the testing of metals, fracture and mechanical tests can be carried out on different materials, such as welded polymers including plastic pipes.

14.3.4 Fatigue Testing

Performed in air or seawater environments, these tests are used to test parent materials and the endurance of welded joints under constant or variable amplitude loading. This destructive testing method can also be used for fatigue crack growth testing of welds, base metals, and heat affected zones.

14.3.5 Hydrogen Testing

This type of testing covers materials that have a risk of corrosion from exposure to hydrogen. These tests can be carried out at a variety of different temperatures and strain rates.

14.3.6 Residual Stress Measurement

Residual stresses are those that remain in a solid material after the original causes of any stresses have been removed. These can be intentional, such as with the scratch-resistant glass on smartphones, or unintentional which can lead to premature failure of a structure. Measurement of residual stresses allows for designers and engineers to determine factors like near-surface and through-thickness residual stress distribution, which can be used in engineering critical assessments.

14.3.7 Test for resistance to attack by hand tools

The tools to be used for attacking the railway infrastructure lock are chisels, tension block, angle grinder, hand hammers, pliers, screwdrivers, wrenches, crowbars and ripping tools (of length not exceeding 1,5 m), lock picking and manipulating devices, and the appropriate portable electric drilling machine, drills, and a sledgehammer, as given in Appendix A.

14.3.7.1 Procedure

14.3.7.1.1 Ensure that the lock is in the normal vertical position and that the hand tools specified in table 1 are used for the appropriate time.

14.3.7.1.2 Allow the test personnel to attack the lock and attempt to make a successful entry by a single method chosen by TRIM after examination of the door.

Respondent's Signature

Date & Company Stamp

14.3.7.1.3 To prove the resistance of the lock under test, the test personnel can make further attacks using the same or other methods of attack, each for the appropriate time.

14.3.7.1.4 Check for compliance with requirements.

14.3.8 Test for resistance to attack by electric disc-cutting machine

Attempt to make a successful entry through the door. Check for compliance with the applicable requirements.

14.3.9 Test for resistance to attack by oxyacetylene cutter.

Oxy-acetylene cutter that has a cutting nozzle of size not exceeding 3 mm and that is used with not more than 11 kg of oxygen and 9 kg of acetylene combined in suitable proportions, in accordance with the requirements of SANS 10238.

14.3.9.1 Procedure

14.3.9.1.1 Attempt to make a successful entry through the door by attacking it with the specified equipment.

14.3.9.1.2 Check for compliance with the applicable requirements.

14.3.10 Test for resistance to attack by diamond core drill

Diamond core drill, as described in Appendix A will be used for this test.

14.3.10.1 Procedure

14.3.10.1.1 Attempt to make a successful entry through the door by attacking it with a diamond core drill.

14.3.10.1.2 Check for compliance with the requirements.

14.3.11 Test for resistance to attack by an impact tool

Portable impact hammer or hammer drill, of size not exceeding 25 mm, and rated at a current of 5 A to 10 A, and a voltage of 230 V to 240 V will be used for this test.

14.3.11.1 Procedure

14.3.11.1.1 Attempt to make a successful entry through the door, by attacking it with a selected tool.

14.3.11.1.2 Check for compliance with the requirements.

Respondent's Signature

Date & Company Stamp

14.3.12 Test for durability of lever locks

Remove the lock from the door, secure the lock rigidly, insert the key, and use a suitable actuating mechanism to turn the key to operate the lock for a total of 30 000 opening-and-closing cycles at a rate of 56 cycles to 65 cycles per minute. Check for compliance with the relevant requirements.

14.3.13 Test for durability of bolt work

With the door or panel upright and in the open position, use an actuating mechanism (attached to the bolt work spindle) to operate the bolts from the fully closed position to the fully open position and back to the fully closed position 30 000 times, at a rate of 15 cycles to 20 cycles opening-and closing cycles per minute. Ensure that approximately the same shock force is applied to the bolts as is applied in normal operation. At the end of the test, examine the bolt work for compliance with the relevant requirement.

14.3.14 Test for corrosion resistance

Use the procedure given in SANS 9227 with an exposure time of 16 hours.

15. QUALITY CONTROL

All equipment as required by various clauses of this specification must be manufactured in an environment that complies with the latest SANS ISO 9001 to ISO 9004 or similar quality control standards. Details must be furnished.

16. LEGAL AND OPERATIONAL

- 16.1 The railway infrastructure lock is to comply with the requirements of this specification, related SANS standards, Safety and Environmental standards in force at the time of tendering.
- 16.2 The information as requested by the various clauses in this specification is to be supplied in form of a technical data, pamphlets and/or drawings. If this is not complied with, offers may be overlooked.
- 16.3 All equipment is to be guaranteed for a minimum period of 24 months against faulty material and poor workmanship - fair wear and tear excluded. Full details of guarantee are to be submitted.

Respondent's Signature

Date & Company Stamp

17. TENDERING PROCEDURE

- 17.1 Tenderers shall indicate clause-by-clause compliance with all specifications as well as the relevant equipment specifications.
- 17.2 The tenderers should fill in a separate document listing all the specifications clause numbers indicating the individual statement of compliance or non-compliance and clarifications.

18. INSPECTION AND QUALITY ASSURANCE

- 18.1 TFR reserves the right to inspect the equipment during or after manufacture and to be represented at any tests.
- 18.2 TFR's staff to ensure the satisfactory operation thereof and for inspection purposes clauses 22.1 of CEE.0019.90.
- 18.3 Should the values measured be below those specified, any subsequent return to site by Transnet staff for further measurements will be to the successful tenderer's account.

19. GUARANTEES AND DEFECTS

- 19.1 The guarantee for good workmanship shall expire after a period of 3 months commencing on the date of completion of the contract or the date the work is handed over to Transnet whichever is the latest.

20. CONTRACT REQUIREMENTS

- 20.1 TFR calls for proposals from experienced bidders with a proven track record of five (05) years to supply, fit, and remove container locking device on containers, rail wagons, and fuel tankers at the areas on the table 2.

Rail Wagons	
<u>Beer Wagons</u>	<u>Sugar Wagons</u>
a. Rosslyn	a. Felixton Mill (KZN North Coast)
b. Nelspruit	b. Amatikulu Mill (KZN North Coast)
c. Bloemfontein	c. Refinery
d. Kimberley	d. Terminal
	e. Bayhead
	f. Maydon Wharf

Respondent's Signature

Date & Company Stamp

		g. Wash out bay
Containers		
<u>Durban</u> a. Kings rest b. Point c. PX depot d. Maydon wharf depot e. Bayhead f. Cato ridge (new) g. Explosive siding	<u>Johannesburg</u> a. Vaalcon Vereeniging b. SACD c. PX Depot (entrance and exit) d. Grindrod e. Bridge 1 & 2 depots f. City Deep / Kaserne • Houer Wessel depot • Kascon • Mark Wessels • West depatures • Middlewerf g. Trichardt h. Natspruit i. MSC Depot	<u>Other areas</u> a. Worcester b. De Aar c. Bloemfontein d. Musina e. Nelspruit f. Kimberley g. Mafikeng h. Richards Bay - Nsese (new) i. Empangeni j. Golela (New)
<u>Port Elizabeth</u> a. Harbour b. Green trees c. Coega d. MSC Depot	<u>Cape Town</u> a. Belcon b. Harbour c. MSC Depot	<u>Pretoria</u> a. Pretcon b. Nissan c. BMW d. Ford
<u>Other Countries</u> a. Lesotho b. Botswana • Gaborone • Francistown • Mahalapye • Palapye • Selebi Pikwe c. Swaziland (new)		
Fuel Tankers		

Respondent's Signature

Date & Company Stamp

a. Central Region b. Western Region c. Eastern Region f. Swaziland Traffic
a. Derailments b. Wagons going off route i.e. sugar and beer wagons, de clamping at places like Piketberg, Malmesbury, etc. c. Any other depot and/or location designated by TFR in consultation with the bidding company. (e.g. Private client sidings)

Table 2: Areas where services are required.

- 20.2 Services will be required on a Twenty-Four (24) Hours a Day / Seven (7) Days a Week / Three Hundred and Sixty-Five (365) Days a Year basis for a period of three (03) years.
- 20.3 The bidder must have at least 10 000 intelligent driven smart container locks available for the purpose of rendering the service in terms of an agreement and ensure the logistics capability to distribute the aforementioned locks amongst the different depots/premises of TFR and meet TFR's requirement to have the cargo containers/rail trucks locked at the designated depots /premises; the minimum number of locks required to service the agreement will be reviewed on a bi-annual basis.
- 20.4 The bidder must supply and fit the lock/s, in fully operational /working condition, on every cargo container/rail truck at depots/premises designated by the TFR or in accordance with the train schedules communicated to the bidding company by TFR from time to time. Cargo containers/rail trucks are to be locked after they have been loaded onto rail trucks.
- 20.5 In respect of point 20.3 above, the bidding company shall supply and fit container locks on all container trains in all channels or railway lines that are designated by TFR and loaded with exposed containers. This will be fitted on all 12 metres containers and in all cases where the 6 metre containers are not loaded door to door.
- 20.6 The bidding company must ensure that the top and bottom of all exposed containers are adequately secured and recorded on the check sheet. The locks must be removed from cargo containers/rail trucks at the locations designated by TFR or in accordance with the train schedules as communicated from time to time. Claims by TFR's customers arising from failure to remove clamps at TFR destination yards will be for the account of the bidding company.
- 20.7 The bidding company shall supply the lock and perform locking and unlocking services. Performance of the Services shall be in a manner most suited to the requirements of the project and where

Respondent's Signature

Date & Company Stamp

appropriate, in accordance with the reasonable instructions as may from time to time be issued by TFR in writing and agreed to by the bidding company.

- 20.8 The bidding company shall ensure timeous liaison with TFRs local Rail Planning Office and its security representative at the respective depots/premises where the containers/rail trucks must be locked or removed to avoid train departure and delivery delays by the bidding company.
- 20.9 The bidding company must ensure that its employees complete the daily Check Sheets properly as approved by TFR in respect of each train from which the locks of containers/rail trucks would have been removed.
- 20.10 The bidding company shall forward all Check Sheets daily via email to a designated official of TFR.
- 20.11 The bidding company undertakes to avail staff (Where required), to provide statements to Transnet or the police or to testify in subsequent Court proceedings in the event of any arrests or internal investigation or proceedings of TFR.
- 20.11 The bidding company will make available information relating to the crime hot spot areas as identified through the crime analysis done. The bidding company further offers its investigations capacity to identify, infiltrate and apprehend criminals' activities associated with theft and attempted theft on clamped containers and cargo.
- 20.12 Further value add can be derived from limiting losses through pro-active investigations and management initiatives that should ultimately result in a reduction in insurance cost whilst at the same time improve confidence in rail transportation from a consumer point of view.
- 20.13 The bidding company must demonstrate its ability to:
- 20.13.1. manage the logistics of the locks at various TFR depots nationally and internationally.
 - 20.13.2 manage the security of the locks (i.e. no unauthorized persons must be in possession or have access of the clamps/locking devices or the mechanisms used to unlock(remove) the locks (such as a key, keycard, fingerprint, RFID card, security token Etc.).
 - 20.13.3 secure and control the issuing and management of clamps/locking device tools. (including the unlocking).
 - 20.13.4 ensure the timeous locking and unlocking of the clamps/locking devices and ensure that the locks are securely in place from train departure to destination.
- 20.14 The bidding company must re-examine the smart locks on a quarterly basis, to ensure the security thereof. The successful respondent should have the research and design capability to continuously improve the design of the lock for the lock to remain effective.
- 20.15 Alternatively, the bidding company shall procure/manufacture improved locks that become available in the market should the locks proposed prove to be ineffective.

Respondent's Signature

Date & Company Stamp

- 20.16 During the contract period, the bidding company shall lock all loaded containers which are found to have exposed doors irrespective of the container size. All empty sugar wagons also need to remain locked due to the nature of the commodity.
- 20.17 The bidding company will not engage in any duties or roles prior to consultation with TFR and subsequent written confirmation is served by TFR.
- 20.18 Submission of investigation reports on all lock related incidents need to be supported with photographs.
- 20.19 The bidding company will be required to enter a performance management contract to measure the success of the freight protection service.
- 20.20 The bidding company must have an Investigation Team to analyse hotspot areas at areas where the smart locks are tampered with or breached.
- 20.21 The bidding company must ensure continuous improvement of the smart lock for the duration of the contract.
- 20.22 The bidding company shall take all measures reasonably necessary to comply with all laws and regulations in force from time to time in any place where the services are to be wholly or partially performed.
- 20.23 The bidding company shall render the services in accordance with the prevailing professional standards.
- 20.24 The bidding company shall provide the services of suitably qualified persons to lead the project. The qualification and experience of the bidding company's qualified persons shall be appropriate and adequate for the purpose of rendering the services.
- 20.25 Such qualified persons shall not be removed from the Project and the rendering of the Services, without the prior written consent of TFR, which consent shall not be unreasonably withheld.
- 20.26 Whenever, for any reason such persons are unavailable for the performance of the Services, the Bidding company shall as soon as reasonably practical, substitute suitably qualified replacements acceptable to TFR, without any additional cost to TFR.
- 20.27 In addition to the qualified persons referred to above, the Bidding company shall provide and supervise such other suitably qualified and competent staff who are necessary for the execution of activities performed by the Bidding company. The Bidding company shall provide TFR with details of the qualifications and experience of the staff provided, as required and upon receipt of a written request for same.

Respondent's Signature

Date & Company Stamp

- 20.28 TFR shall have the right to require services from the Bidding company, by notice in writing, to immediately remove any person whose continued presence on the Project is, in the reasonable opinion of TFR, undesirable and/or unnecessary. The Bidding company shall, if so, required by TFR as soon as reasonably practical, replace any person so removed with a person of equivalent qualifications and skill.
- 20.29 The Bidding company and its suitably qualified persons, who are rendering services to TFR in terms of this agreement shall, for the duration of this agreement, be screened for criminal records and registered in terms of the PSIRA Act. No 56 of 2001 and shall comply with the provisions of the Code of Conduct issued in terms of the said Act.
- 20.30 The Bidding company shall ensure that its employees involved in the rendering of Services in terms of this agreement shall attend, if necessary, Court proceedings as well as disciplinary and arbitration proceedings should TFR deem it necessary, provided that TFR has notified the Bidding company within a reasonable time before the commencement of such proceedings that the presence of the Bidding company's employees is/are required to attend such proceedings.
- 20.31 The Bidding company shall perform the Services. Performance of the Services shall be in a manner most suited to the requirements of the project and where appropriate, in accordance with the reasonable instructions as may from time to time be issued by TFR in writing and agreed to by the Bidding company.

21. COMPLIANCE AND STANDARDS

- 21.1 The bidding company shall submit the following documents as mandatory returnable documents. Compliance with all applicable legislation shall be at the bidding company's cost. The bidding company shall be liable for any breach by any one or more of its security officers, employees, servants, permitted agents, and bidding company (independent or otherwise) of the provisions of these clauses and hereby indemnifies and holds TFR harmless against all claims, loss, or damage which TFR may suffer arising out of all such breaches.

N.B: All submitted documents and certificates must be valid on the closing date and time of the bid.

Respondent's Signature

Date & Company Stamp

- 21.1.1 The bidding company shall provide a valid PSIRA certificate as a security provider in line terms of section 20 of the PSIRA Act. ("New Certificate" in line with industry circular issued by PSIRA on 10 March 2015). The SSP shall ensure that it obtains and retains its PSIRA registration certificate. The PSIRA certificate must be valid on the closing date and time of the bid.
- 21.1.2 The bidding company shall provide proof of Public Liability Insurance (PLI) cover/or Letter Of Intent (LOI) from Insurer for PLI cover and Third-Party Liability cover for not less than R5 000 000,00 (Five million South African Rand) and with an annual limit cover of not less than R30 000 000,00 (Thirty million South African Rand).
- 21.1.3 The bidding company shall submit a confirmation of registration from the Security Industry Provident Fund.
- 21.1.4 The bidding company shall submit a letter of Good standing from PSIRA.
- 21.1.5 The bidding company shall provide valid proof of PSIRA (Minimum Grade B credentials for each Member (Director, Partner, Trustee) of the bidding company. The PSIRA certificate must be valid on the closing date and time of the bid.
- 21.1.6 The bidding company shall submit Criminal clearance certificate/s for all Company Directors and/or Shareholders. Only the criminal clearance certificates issued by the South African Police Services (SAPS) will be accepted.
- 21.1.7 The bidding company shall submit a valid and signed Letter of good standing from PSIRA. The letter of good standing shall be on PSIRA letterhead.
- 21.1.8 The bidding company shall submit a signed Letter of Good Standing from the Compensation fund for Occupational Injuries and Diseases Act (COIDA).
- 21.1.9 The bidding company's personnel must be registered with PSIRA. The bidding company shall submit valid PSIRA registration certificates (Minimum Grade B and C) of at least five (5) personnel currently employed by the bidding company to prove compliance.

Respondent's Signature

Date & Company Stamp

21.1.10 The bidding company's personnel must be criminally vetted and issued with South African Police Service- Criminal Clearance Certificate. Submission of the security clearances from other institutions will not be accepted and will lead to disqualification. Vetting shall be maintained through annual and periodic vetting processes. The bidding company shall submit the SAPS Clearance certificates of at least Five (5) security officers employed by the bidding company for the same employees as stipulated in 7.1.9 above. The clearance certificates shall be in line with the Schedule Table of Offences, of the Private Security Industry Regulation Act 56 of 2001.

22. COMPLIANCE WITH STATUTES

22.1 The Bidder shall comply with all relevant legislation as amended from time to time, including, but not limited to the ones below. Compliance with all applicable legislation shall be at the Bidder's cost.

22.1.1 PSIRA Act (56 of 2001), as amended;

22.1.2 Private Security Industry Levies Act, (23 of 2002);

22.1.3 National Key Points Act (102 of 1980), as amended;

22.1.4 Basic Conditions of Employment Act (75 of 1997);

22.1.5 Compensation for Occupational Injuries and Diseases Act (130 of 1993), as amended;

22.1.6 Provincial ordinances and laws and municipality by-laws including all relevant regulations promulgated;

22.1.7 The Occupational Health and Safety Act (83 of 1993);

22.1.8 Protection of Personal Information Act (4 of 2013);

22.1.9 Firearms Control Act, (60 of 2000), as amended;

22.1.10 Criminal Procedure Act (51 of 1977);

22.1.11 Control of Access to Public Premises and Vehicles Act (53 of 1985), as amended;

22.1.12 Codes of Good Practice embodied in the Broad Based Black Economic Empowerment Act (53 of 2003);

22.1.13 Independent Communications Authority of South Africa Act (13 of 2000), as amended;

22.1.14 Legal Succession to the South African Transport Services Act (9 of 1989);

22.1.15 Income Tax Act (52 of 1962);

22.1.16 Value-added Tax Act (89 of 1991);

22.1.17 Trespass Act (6 of 59)

22.1.18 Criminal Matters Amendment Act (18 of 2015);

Respondent's Signature

Date & Company Stamp

22.1.19 Any other legislation and regulations and/or in-house specific policies, procedures guidelines that govern some of TFR's sites; and

22.1.20 Any other regulatory obligation such as the Railway Safety Regulator (RSR) Act (16 of 2002).

23. DOCUMENTS PROPERTY OF CLIENT

23.1 Bidders are reminded that all drawings and specifications issued to them are the property of the CLIENT and must be returned to the CLIENT whether a tender is submitted or not. Designs, drawings, etc. supplied by the contractor for the provision of this service will be the property of the Client, and therefore should not be reproduced nor moved to third parties.

Respondent's Signature

Date & Company Stamp