TECHNICAL ASSISTANCE (TA) FOR THE EASTERN AND SOUTHERN AFRICA (EA-SA) TRANSPORT AND TRANSIT FACILITATION PROGRAMME (TTTFP)

Ref. EuropeAid/138372/IH/SER/MULTI

RFS N. 2015/367563

CONTRACTING AUTHORITY:

SOUTHERN AFRICA DEVELOPMENT COMMUNITY (SADC)

TRS-002-001

Hosting Requirements for the Tripartite Transport Registers and Information Platform System (TRIPS)

August 2019

TABLE OF CONTENTS

LIST OF DEFINITIONS, ACRONYMS AND ABBREVIATIONS

DR   : Disaster Recovery

ISP   : Internet Service Provider

NTIS   : National Transport Information System

SAN   : Storage Area Network

TA   : Technical Assistance

TRIPS   : Transport Registers and Information Platform System

TTTFP   : Tripartite Transport and Transit Facilitation Programme

VM   : Virtual Machine

AMENDMENT HISTORY

When the last revision of this document (as shown below by the revision and date) has been authorised and distributed, all previous issues are to be disposed of.

Revision	Item	Paragraph	Description	Date
0.1			Initial Release	01/08/2019

A.   INTRODUCTION

This document was prepared in response to Technical Assistance (TA) number 0172 under the Tripartite Transport and Transit Facilitation Programme (TTTFP).

1.   OBJECTIVE

The overall strategic objective of this assignment is to facilitate the development of a more competitive, integrated and liberalised regional road transport market in the tripartite region.

The specific objective and key result area that this assignment contributes to is KR3: Preconditions for an operational tripartite Transport Registers and Information Platform System (TRIPS) implemented.

2.   PURPOSE

The primary purpose of TRIPS is to improve access to information between participating Member/Partner States. TRIPS will act as a gateway among the 25 participating continental Member/Partner States of the Tripartite. A Member/Partner State will thus be required to only develop interfaces to TRIPS rather than to the National Transport Information Systems (and related modules) of all other participating Member/Partner States.

The purpose of this document is to define the requirements for hosting, operating and physically housing the hardware together with the TRIPS application software and international internet connectivity.

3.   DISTRIBUTED HOSTING

The final installation objective is to connect TRIPS to the National Transport Information Systems (NTIS) of the 25 participating Member/Partner States. If TRIPS is hosted at a single location, an interruption in internet connectivity to that location will interrupt the intracontinental operation of the TRIPS system too. Therefore, it is recommended that TRIPS must be hosted in at least two locations to enable connectivity to different international internet services, with each client Member/Partner State connecting to the TRIPS host closest to them and using the other TRIPS host as a fall-back to ensure constant operation. To facilitate this redundancy, live replication of the request record database is required.

Furthermore, in the interest of providing rapid recovery in case of a catastrophic failure at one of the sites, it is recommended that an off-line disaster recovery (DR) system be hosted at a third, geographically separate location from the two hosting sites, if such a site can be accommodated in the budget. Periodic backups of database from one of the hosting sites must be made to this location, although each host would have the capability to backups. Snapshots of virtual machines from both locations should also be stored at the DR site. In case of a failure of one of the hosting sites, all TRIPS communications will be diverted to the remaining site while the failed site will be repaired using the backups from the DR site.

It is recommended that the DR site should not be combined with one of the hosting sites, for if one host should fail, recovery will be slowed down significantly as the backups have to be obtained from the remaining host, which would then be handling all TRIPS communications. The configuration is shown in TRS-003: *Hardware, System Software and Ancillary Equipment Specification for the Tripartite Transport Registers and Information Platform System (TRIPS).*

B. HOSTING REQUIREMENTS

TRIPS will be hosted at a total of three locations: Two locations will host TRIPS itself, while a third will host the DR site. The locations where the TRIPS and DR servers are hosted will have to provide facilities complying with the requirements described in the following sections.

1. SERVER HOUSING REQUIREMENTS

The following requirements pertain to the physical environment in which the servers will be housed.

- The server room must have a raised floor to facilitate cabling and power supply to the equipment;

- The server room ceiling must be at least 2.75 metres above the raised floor and have no cavities extending beyond the walls of the server room;

- The server room or section of the server room dedicated to hosting the TRIPS should be of at least 12 m^2 to house all equipment as specified in TRS-003 and provide enough room for staff to operate in;

- The server room must be properly insulated and provide an air-conditioning system (with redundant backup) to maintain the server room ambient temperature between 20° to 24°C and the ambient relative humidity levels between 45% and 55% at all times;

- The server room must be constructed using fire/flame retardant material (door, floor, ceiling, insulation, etc.) and be equipped with automated fire suppression systems using FM200 Gas;

- The server room must be equipped with environment condition (temperature, humidity, etc.) monitoring systems that can be connected to the servers to initiate a shutdown in the event that the temperature or other environmental conditions deviate outside the specified limits to prevent damage to the components of the servers; and

- The facility must comply with all occupational health and safety requirements of the host Member/Partner State, if these are compliant with international standards.

2. OPERATIONAL REQUIREMENTS

These requirements address those factors that can influence the operation of the site.

- The facility must be able to provide secure remote access to developers and maintenance personnel;

- The facility should be accessible within half a day's travel from an international airport;

- The facility should be equipped with land lines with the capability of receiving and making international calls;

- The facility should have continuous and good cell phone reception;

- The facility should have access to an email server which is completely separated from any TRIPS servers;

- The facility should have sufficient nearby accommodation for housing the installation team and maintenance personnel; and

- The facility must be accessible by the relevant hardware distribution channels that carry sufficient maintenance/replacement stock to honour warranties and service level agreements and have certified capability to service the equipment.

3.   SECURITY REQUIREMENTS

These requirements pertain to the physical and virtual security provided by the facility.

- The facility in which the server room is housed must be located in a building or complex where threats such as labour or civil unrest will not place the operation of the system at risk;

- The facility should be equipped with biometric access control system to restrict access to the servers by the authorised staff members only;

- The server room must have a solid fire proof door secured with a second layer of access control;

- The server room must have solid brick walls;

- The server room must not have any windows;

- The facility must provide intrusion and denial-of-service attack detection and mediation software;

- The facility should provide resource monitoring and tamper detection;

- The facility must be equipped with next generation firewall technology with purpose-built security processors, threat intelligence security services, full visibility into applications, users and networks and best of breed security;

- The firewall system must have a comprehensive security portfolio as well as third-party security solutions in a multivendor environment to share threat intelligence and improve security posture;

- The facility must be equipped with anti-virus and malware scanning software;

- The facility must have adequate security protocols in place that access can be revoked if a staff member has been retrenched or deemed a safety risk;

- The facility should vet all personnel employed and maintain records on staff;

- The facility should maintain adequate documentation and training protocols that ensure handover of staff tasks with minimum impact.

■ The facility must enact periodic and surprise audits to check that operating standards are maintained and to ensure compliance with policies and procedures, such as routine backups; and

■ The facility must enact event notification plans in case of security breaches or failures to enable communication of such events to support personnel and users of the system.

4. INTERNET CONNECTIVITY REQUIREMENTS

As TRIPS is at its core an internet application, the requirements involving internet connectivity are of high importance. The hosting locations shall have access to two different sets of international (undersea) internet fibre optic cables for redundancy.

■ The facility must a connection to a broadband internet service provider (ISP) with a speed of at least 10 Mb/s up and down load. The bandwidth is required to simultaneously allow real-time database replication between the TRIPS hosts, regular backups to the DR site and the packet transmissions required for system operation;

■ For each of the TRIPS host sites, the facility must have at least two connections to two different ISPs for redundancy using two different fibre optic cables. If two different fibre optic cables are not available, a different medium (such as wireless) can be used;

■ The facility must contract ISPs that have the capacity to provide increased bandwidth capacity if the requirements of the system change as more countries interface with TRIPS;

■ The facility must have internet connectivity with a 99.9% uptime guarantee.

Based on the configuration of undersea internet cables connectivity to Africa shown in Figure 1 below, it is recommended that the location of the two TRIPS hosting sites have access to the undersea internet cables along the East and West Coasts of the Tripartite Region.
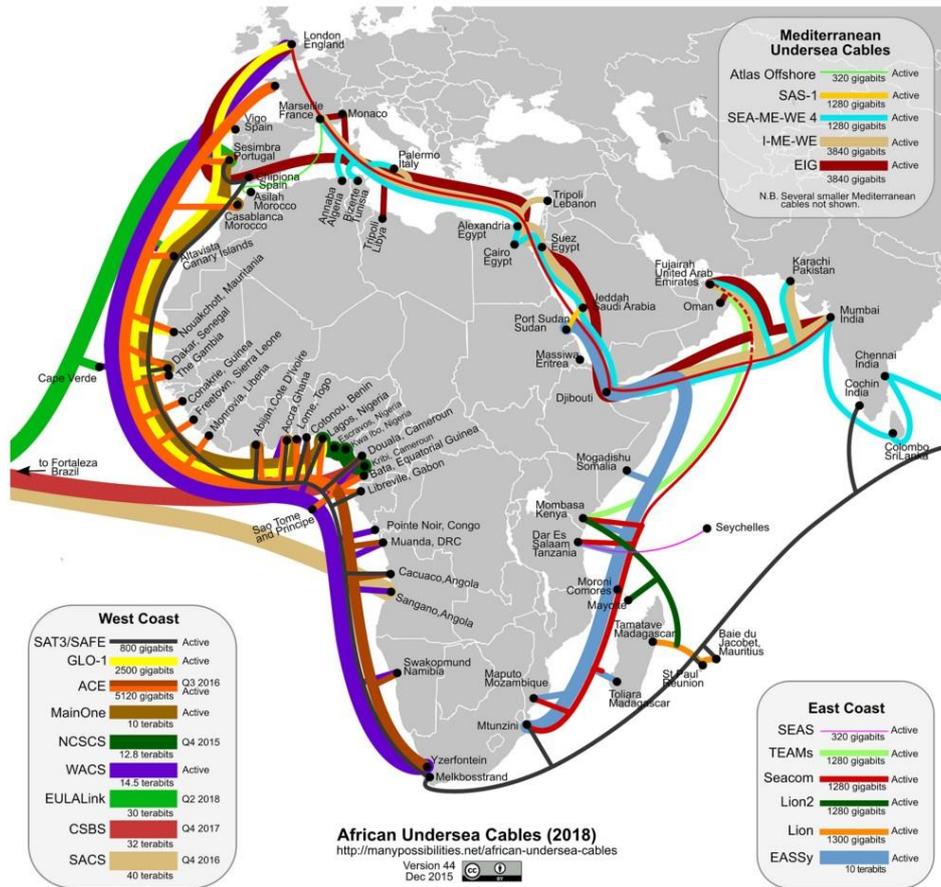
Figure 1. Map of undersea international internet fibre optic cables connecting to Africa (ManyPossibilities.net)

5. REDUNDANCY REQUIREMENTS

TRIPS must operate as a high-availability system.

- The facility must have access to a reliable electrical power grid;

- The facility must have access to a backup power source, such a diesel generator, that can provide sufficient power for a power outage in the host Member/Partner State. The backup power source must be start automatically when a power outage occurs and must have sufficient capacity to continue running until the power is restored, even under circumstances where an extended outage of a week or longer occurs;

- The facility must have the capability to recover, using local backups, from non-catastrophic system failures within 24 hours;

- The facility must have the capability to recover from a catastrophic failure, using backups retrieved from the DR site, within seven days;

- Each facility must maintain the following data backup policy:

  - Incremental backups on a daily basis;

  - Backing up the full database on a weekly basis;

  - Retain the backups of the last three months;

- A host facility must complete a full backup of the database to the DR site on a weekly basis; and

- The DR facility must maintain full backups of the replicated database for the last three months.

6.   STAFFING

6.1. Requirements

The facility staff are fundamental to operating the site according to the prescribed policies.

- Facility staff should timeously and clearly communicate any issues to the service providers responsible for the warranty and support of the equipment or the TRIPS application service provider and provide adequate feedback when completing instructions; and

- Training will be provided to the facility staff in respect of the TRIPS application, equipment and configuration. As a prerequisite for such training facility staff must be adequately trained, be knowledgeable or have capacity on the following:

  - Advanced English language and English ICT technical terminology capability to enable a clear understanding of the system and clear communication with the service providers and users;

  - Enterprise Linux server administration;

  - Certification management using OpenSSL;

  - Database administration and management for SQL Server;

  - Virtual machine management;

  - Network management;

  - Data centre management and operation;

  - Firewall maintenance and administration;

  - System monitoring for detection of intrusions, aberrations and outliers;

  - Advanced security;

  - User access auditing and control;

  - Maintaining and renewing software licences.

6.2. Institutional Structure

The staff and facility must be able to provide support for 24 hours a day, using a shift procedure and/or a standby procedure outside normal office hours (weekends and public holidays included) to deliver the required 24x7 hosting service.

The facility must have a single person in the form of a Hosting Service Manager in charge who takes full responsibility for the functioning of the site, through adequate delegation to supporting staff members.

Reporting to the Hosting Service Manager are the Team Leaders of the 4 support groups responsible for the day to day service. These groups are comprised as follow:
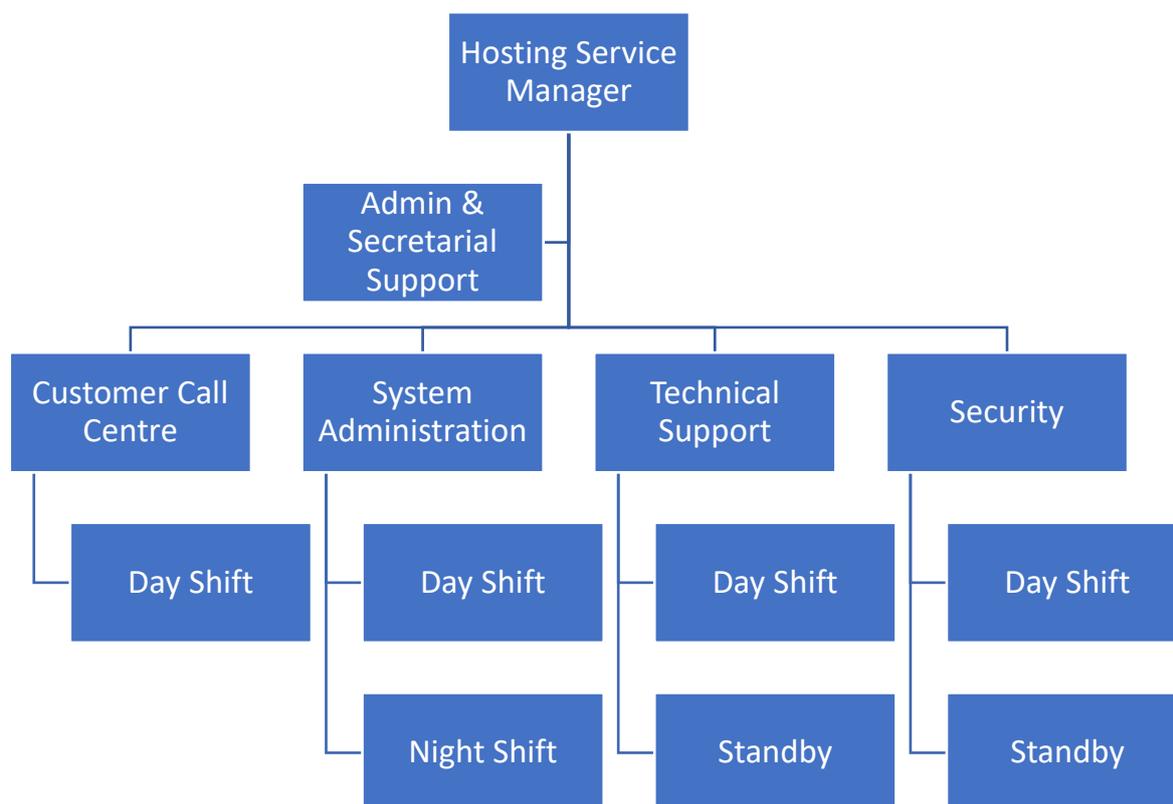
Customer Call Centre: When an interruption in the TRIPS service is experienced by a Member/Partner State, the responsible IT staff of that Member/Partner State would notify the customer call centre of the interruption together with technical information relating to the interruption in service.

System Administration: This group is responsible for the day to day system administration services, including the monitoring of the performance of the servers, storage devices and network connections. Tasks such as the making of back-ups, restoring of back-ups and regular testing of backups are also performed by this group of staff.

Technical Support: The technical specialists with the pre-requisite technical capacity relating to the server operating system, virtual machine configuration, data base management system and network management form part of this group. They are typically on duty during office hours only, but on standby should the system administrators need their special skills after hours for remedial action when a deviation from the operating parameters by a component of the system is observed.

Security: A separate group of technical specialists that are responsible for maintaining the overall physical and virtual security of the facility. This group would be on duty only during office hours, during which they would ensure the firewall is working as it should, ensure that the system is protected against the latest malware developments, maintain the security certificates and provide assistance with other access and security issues. The group should also be on standby outside of office hours should the system administrators become aware of an intrusion or an issue regarding one of the security components of the system.

The following institutional structure is envisaged:

```
                    ┌──────────────────┐
                    │ Hosting Service  │
                    │     Manager      │
                    └──────────────────┘
          ┌──────────────────┐       │
          │     Admin &      │───────┤
          │   Secretarial    │       │
          │     Support      │       │
          └──────────────────┘       │
    ┌──────────┬──────────────┬──────────────┬──────────┐
┌─────────┐ ┌─────────────┐ ┌───────────┐ ┌──────────┐
│Customer │ │   System    │ │ Technical │ │ Security │
│  Call   │ │Administration│ │ Support   │ │          │
│ Centre  │ │             │ │           │ │          │
└─────────┘ └─────────────┘ └───────────┘ └──────────┘
    │             │               │             │
┌─────────┐ ┌─────────────┐ ┌───────────┐ ┌──────────┐
│Day Shift│ │  Day Shift  │ │ Day Shift │ │Day Shift │
└─────────┘ └─────────────┘ └───────────┘ └──────────┘
            ┌─────────────┐ ┌───────────┐ ┌──────────┐
            │ Night Shift │ │  Standby  │ │ Standby  │
            └─────────────┘ └───────────┘ └──────────┘
```

C. EVALUATION REQUIREMENTS

Evaluation of the offers submitted by the Member/Partner States will be assessed in accordance with the requirements in this section.

1. CRITERIA

The Hosting Offer with the highest number of points will be selected as Host Site 1.

Should the Hosting Offer with the second highest number of points be connecting to a <u>different under sea international internet cable</u> than the Host Site 1, this offer will be selected as Host Site 2. Should the Hosting Offer with the second highest number of points be connecting to the <u>same under sea international internet cable</u> than the Host Site 1, the Hosting Offer with the next highest number of points connecting to a <u>different under sea international internet cable</u> than the Host Site 1will be selected as Host Site 2.

The DR Site (if feasible within the available budget) will be awarded to the offer with the highest points after Host Site 1 and 2.

Description	Maximum Points	Awarded Points
Compliance with the Server Housing Requirements	20	
Compliance with Operational Requirements	20	
Compliance with Internet Connectivity Requirements	20	
Compliance with Redundancy Requirements	20	
Compliance with Staffing Requirements & Institutional Structure	20	
TOTAL	**100**	
Additional bonus points to be added to total score for offers exceeding the minimum requirements	10	

2.   DOCUMENTS TO BE SUBMITTED

The following documents are to be submitted in accordance with the evaluation criteria listed above:

Description	√ Tick if submitted
Description, drawings and photographs (if available) of Server Room and required facilities	
Description and procedure manuals of Operational Procedures	
Description and supporting ISP documentation confirming Internet Connectivity	
Description of back-up administration and storage, together with specification and photographs of generator (if available) in compliance with Redundancy Requirements	
Job descriptions, institutional structure and CVs of qualified Staff Members	
Supporting documentation/evidence towards offers exceeding minimum requirements	

3.   ROAD MAP

The road map for the selection of the hosting Member/Partner States is as follow:

#	DESCRIPTION	DURATION	TARGET DATE
1	Validation of TRIPS Specifications and Hosting Requirements by all Tripartite Member/Partner States		6-8 Aug 2019
2	Publish Hosting Requirements on COMESA, EAC & SADC Websites and invite Tripartite Member/Partner States to submit Hosting Offers	4 Weeks	19 Aug 2019
3	Submission of Hosting Offers by Tripartite Member/Partner States		13 Sep 2019
4	Adjudication of Hosting Offers received	3 Weeks	4 Oct 2019
5	Publish details of the successful Hosting Member/Partner States		11 Oct 2019