**SARS RFP 08-2022**

**SARS TECHNICAL SECURITY TENDER FOR THE PROCUREMENT OF :**

**CENTRALISED ACCESS CONTROL SOLUTIONS, INCLUDING MAINTENANCE FOR A PERIOD OF THREE YEARS**

**BUSINESS REQUIREMENTS SPECIFICATION**

**Introduction**

The South African Revenue Service (SARS) has approximately of one hundred and fifty (150) offices (SARS Sites) nationally. The protection of SARS’s assets, people, and general physical security at SARS Sites is of pivotal importance due to the nature of the operations and activities of SARS. The successful Bidder(s) will be required to design, supply, test and commission a scalable smart access control system which incorporates SARS stated devices and equipment like doors, turnstiles, biometric readers, door controllers and closers, vehicle barriers, metal detectors. The integrated access control system must have a capability to integrate, unify and or share information with other SARS specified systems. Additionally, provide SARS with a maintenance and support proposal for a period of three (3) years from the expiry of the equipment warranty. The information collected through the system must be converged from a facility level to regional and national. See Figure 1. For logistical reasons, management and maintenance of the Services, SARS divided the SARS Sites Access Control Servers into **five (5) regions** as shown in the table below.

**Table 1A**

|  |  |
| --- | --- |
| **Region A** | * T1 Server * Gauteng and Mpumalanga Provinces |
| **Region B** | * T2 Server * Limpopo and Northwest. * Including Klerksdorp |
| **Region C** | * T3 Server * Free State |
| **Region D** | T4 Server   * Western Cape and Northern Cape |
| **Region E** | T5 Server   * KZN and Eastern Cape Provinces |

**Smart Access Control System**

SARS seeks to procure a smart, efficient, and reliable access control system that has an ability to integrate, unify and share information with other SARS systems such as:

* CCTV
* Fire Alarm
* Physical Security Guard Patrol System
* Human Resource
* IT (For equipment info such as Laptops, PCs, Projectors, etc)
* Parking system
  + SARS Staff and Visitors
* Environmental systems:
  + Building management
  + Health and Safety, evacuation and converge with security barriers such as boom gates, turnstiles.

**Access Control System Key Features and Capabilities**

SARS seek to procure an access control system which will be used to manage access into and exit from its facilities (including storage facility) for employees, visitors, contractors, vehicles and assets. A component of the system will be utilised only at defined facilities and areas as a time and attendance system. The supply of the access control system includes supply and replacement of readers, maglocks, door closer and sensors to meet SARS defined requirements for each door.

The bidder must provide a warranty for the access control systems in line with the OEM specification of no less than twelve (12) months from date of commissioning and all its components.

The bidder must further submit a maintenance and support proposal including spare parts, monthly maintenance service and call out fees for a period of three (3) years from the expiry of the bidder’s warranty period for each component of the access control system.

The Bidder must train SARS users and supply manuals and certification where possible

* + System Admin
  + Maintenance team
  + System Operators
  + Management

In addition, SARS promotes agility between facilities countrywide specifically in accessing physical spaces for staff members, contractors, and visitors. The proposed access control system is required to have the ability to:

* Design and deliver a web-based App for the access control system to facilitate the pre-registration of personnel and vehicles for access, send sms and emails as per SARS’s requirement
* Have a Web-Based Access Control interface.
* Remotely accessible with software installed in laptops of our responsible system personnel, e.g. Technical Security Technicians, System Administrators, Regional Security Managers and Access Control Data Capturers.
* Set up Administrator and End-User profiles with different access levels.
* Multiple access to the system with no interruptions.
* Single National Database for all SARS sites, including Ports of Entry, Branch Operations and Customs Offices.
* The database must be profile based instead of card-based, then an access card is attached to the profile and buildings’ access added as required.
* The proposed system support remote management and a centralised SQL database
* Adherence to SARS Enterprise IT architecture software standards.
* SARS requires a flexible and expandable access control system that has an ability to incorporate a series of devices such as but not limited to (access cards, biometric, electronic keys, electronic Occurrence Book)
* Real time Main Activity transaction logs.
* Reconfigured site mapping according to individual site and business unit requirements.
* Live Site maps displaying all controllers and their status.
* Send alerts and notifications to Security System administrators, control room of any arising system failure and faults to enable a prompt response.
* To do headcount as access cards tag through the readers.
* The access control system must provide for web-based applications through an App and further provide for authorisation through the App by authorised End-Users.
* The information on the App must be stored within the system to provide for operational outcomes and audit trail.
* Record each access application, transaction, termination be kept in the building and centrally.
* Allow for pre-registration of visitors through a web-based Application. A SARS visitor, contractors and staff member must be authorised access online or at access control self-processing kiosk.
* Do automatic daily backups and store in the regional server and national server.
* Support network and cloud storage.
* Have the ability to back-up on IBM DS storage management drives or back up servers, regional storage and both centralised.
* The system must have the ability to integrate with other organisational access devices like facial reader with unmanned fixed temperature screening and contactless wave readers.
* The door controllers must have ITC/IP capability
* Interface with electric locks, door sensors, break glass units
* Configure commands for system desired functionality dependant on site. E.g, set times for doors to be inaccessible and anti-pass backs.
* The proposed access control system must be fully functional, door controllers and readers even when the main server is offline.
* Seamlessly integrate and interface to other systems to exchange information with third-party systems, allowing SARS to automate access decisions and proactively manage site access from one software platform.
* Evacuation and building exit doors to sense and do specific head count during emergency alarms using a Quick Response sensor.
* Be scalable up and downwards with minimal or no effect to the rest of the system that is running.
* The system must record details of lost, stolen, disabled, expired or active cards or biometric data against individuals thereby providing irrefutable audit trail.
* The system must provide for an undisputable audit trail.
* The proposed system to have asset tracking capability for laptop and other electronic equipment, like Cameras; Projectors, etc in an individual’s access control profile and be able to scan barcode and block or grant access.
* Provide the ability to use tablets/ laptops with a wireless reader
* Access control will be utilised for external and internal environments
* The system must be capable to provide management with SARS defined reports (real time and historical reports) at a facility, regional and national level
* The service provider must specify the licence structure of the proposed access control system, preferably an enterprise licence
* The access control system must have the capability to converge at the monitoring station at facility, regional and national level for monitoring events at SARS designated control room(s) real time and historical.

The access control should have the capability to schedule and conveniently configure to control access to rooms, areas and buildings

The access control must facilitate swift entry and exit between building areas and SARS buildings as approved.

**Employee Verification Capability**

SARS utilises three access principles i.e. what you are, what you have and what you know. At any given time, the access control system must be able to use a combination of two of the principles, dependant on the building protection objectives. SARS requires an access control system that has a verification capability which consist of but not limited to the following:

* Card Reader
* Biometric
* Pin Code
* Number Plate Recognition

The bidders proposed system must demonstrate the functionality of the above-mentioned inputs, the management of cardholder access, biometric credentials, card and photo identification, and record any number of personal data fields against individuals for easy access to information.

**Visitors and Contractor Management Systems**

The Access control system must be able to manage contractors and visitors to SARS sites via the command-and-control systems.

* Manage and control access for visitors with extensive pre-registration and reception-based functionality. APP)
* The facility system must send a notice to the host and security to client monitoring system 30 min before visitor expiry times
* The proposed system at a facility level must send a notice to Manager and security at client monitoring system 30 min before visitor expiry times
* Notify the host or escort via email or SMS when a visitor arrives. Host then approves and collect the visitor. Host is responsible for that visitor until they exit SARS premises.
* The proposed system must notify the host to receive an SMS and email when their visitor is still in the SARS premises after hours.
* Quickly identify pre-registered visitors using QR.
* Efficiently entry and exit reporting to help reconcile contractor time on site against what is invoiced.
* Issue Mobile Connect credentials (log-in) into the App from Visitor Management
* For returning visitors, previously stored details can be retrieved
* Automated sign-in using information retrieved from a licence and ID card The App must send an sms with a number for the visitor for access parking or office park
* Configurable inclusion of privacy statements or conditions of site entry
* Visitor induction using supplied material.
* Physical Security personnel to assist visitors in using the Kiosk.

**Reception Workstation**

Visitor Management provides a targeted user interface for a receptionist managing visitors onto and off-site, including updating visitor details, capturing photos and printing visitor labels, assigning escorts, a card and visitor access. The reception client supports manual or automated email/SMS notifications to hosts of visitor arrival or visitors who are overdue to leave. Additional reception features include:

* Pre-registration of visits with automatic re-use of visitor details recorded on a prior visit
* Support for multiple visitors on a single visit to reduce repetition of data entry
* Flexible configuration of visitor details, based on visitor type
* Reception home screen displays visitors by status: expected currently on-site, due to leave, overdue to leave, temporarily offsite or visitors who have already left
* Bulk selection and processing of visitors, for example, to preprint visitor labels at the start of the day or to check on-site a bus load of visitors arriving together
* Enrolment of visitor fingerprints for site access and visitor identification
* Up to five pre-configured macro buttons to initiate actions such as printing an evacuation report, locking down the front door or triggering a silent alarm
* Support for multiple receptionists manning a single reception point, as well as sites with many distributed reception points
* Visitor reporting including the current status of visitors expected or on-site today and summary reports on visitor and escort past and planned visits.

**Self-Registration Kiosk**

The access control system must be able to facilitate Self-Registration Kiosk that integrates seamlessly with the Visitor Management workstation, allowing sites to share host, visit and visitor configuration so that visitors arriving on-site can be managed from either a reception workstation or a Kiosk. The Kiosk must allow visitors to sign-in for a visit independently of the receptionist.

On completion of sign-in their host must be automatically notified of their visitor’s arrival via email or SMS.

Hosts must be able to manage their visitors on and off-site from the Kiosk in line with the access permissions of a visitor as per security set access levels, update the visit details or reprint visitor labels.

Hosts of visitors who are overdue to leave must automatically notified for follow-up action.

**System Integration, Unification and Data Sharing**

The access control should integrate with HR systems via a command control system to enable simple and efficient management of staff and contractors. Security Systems to have only limited necessary access to HR information.

A quick link to be created on the ESS Portal for Access Control Application which will link to your reporting Line Manager for approval.

**Access control information flow:**

* HR captures new employee.
* Trigger sent to the Access Control Data Capturing team.
* Pre-populated information pops-up on the access control software with specifics of individual’s Functional Unit, Base site and Line Manager.

**Storage of information:**

At door level, the site controllers must have individual information stored on the PC board. Regional servers will also mirror that information as well as a centralised Main Server.

* Duration of information storage:
  + Two types of information:
    - Employee Profile to be kept while you are at SARS service and 5 years after service termination.
    - Storing of information for visitors and contractors
    - Activity which needs to be available from the very first tag until 5 years after service termination.

Failure of the system and how information should be stored at door level, area, facility and centrally

**Existing Staff access requirements:**

* Online application via ESS Portal(SARS Platform)
* Manager’s approval

**Contractor access requirements:**

Two types of contractors:

* Ones who have full access to SARS Intranet systems can do it online.
* External Service providers with no access to the SARS Intranet:
  + Site Monitor to assist.
  + Complete Online Application and get approval.
  + Attach ID copy

Automatic fault report of access control and integration with SARS remedy system

**Backup power**:

The system equipment will need two phases of backup power. Onboard battery inside each controller box.

* The access control system will also be connected to a Double Conversion / Online UPS and generator power.