



**BID SPECIFICATION**

|  |  |
| --- | --- |
| **RFQ No:** | RFB 3139/2025 |
| **Description** | The Appointment of a Service Provider for the Planning, Design, Supply, Installation and Configurations of a Total Network Access Control (NAC) Solution with Maintenance and Support for the Period of Five (5) Years. |
| **Issue Date** | 19 August 2025 |
| **Non-Compulsory Virtual Briefing** | 26 August 2025  Time: 10:30 am – 12:30 pm (South African Time)  Venue: Microsoft Teams  [**Join the meeting now**](https://teams.microsoft.com/l/meetup-join/19%3ameeting_ZGQ0MmRhMjgtMDRkMi00MGEwLWJhYmMtNzI0NWJlNTY2MTdh%40thread.v2/0?context=%7b%22Tid%22%3a%2248cd5724-88c7-48c3-a665-945436edd7fc%22%2c%22Oid%22%3a%227a6dc39b-1322-42f5-8168-0d141cfc9019%22%7d) **(right click on join the meeting now, select open hyperlink to join the meeting)**  Meeting ID: 329 058 159 691 8  Passcode: fm6WE6hw |
| **Closing Date for questions / queries** | 29 August 2025 |
| **Bid Response Submission Address** | **Tender Office**  459 Tsitsa Street, Erasmuskloof, Pretoria, 0105 |
| **RFQ Closing Details and Time** | Date: 12 September 2025  Time: 11:00 (South African Time) |
| **RFQ Validity Period** | 200 Days from the Closing Date |

**NOTE: PROSPECTIVE BIDDERS MUST BE REGISTERED ON NATIONAL TREASURY’S CENTRAL**

**SUPPLIER DATABASE (CSD) PRIOR TO SUBMITTING BIDS.**

Contents

[1. Purpose and Background 3](#_Toc203031548)

[2. Scope of Bid 3](#_Toc203031549)

[3. Product / Service Requirements 4](#_Toc203031550)

[3.2 Special Requirements 6](#_Toc203031551)

[4. Bid Evaluation Stages 6](#_Toc203031552)

[4.1 Mandatory Administrative Responsiveness (Stage 1) 6](#_Toc203031553)

[4.1.1 Attendance of briefing session 6](#_Toc203031554)

[4.1.2 Registered Supplier 6](#_Toc203031555)

[4.1.3 Bid Submission Instructions 6](#_Toc203031556)

[4.2 Technical returnable documents 7](#_Toc203031557)

[4.2.1 Instruction and evaluation criteria 7](#_Toc203031558)

[4.2.2 Technical Mandatory Requirements (Stage 2) 8](#_Toc203031559)

[4.3 Special Conditions of Contract Verification (Stage 3) 11](#_Toc203031560)

[4.3.1 Special Conditions of Contract 11](#_Toc203031561)

[4.3.2 Contracting Conditions 11](#_Toc203031562)

[4.3.3 Delivery Address 11](#_Toc203031563)

[4.3.4 Services and Performance Metrics 11](#_Toc203031564)

[4.3.5 Supplier Performance Reporting 11](#_Toc203031565)

[4.3.6 Certification, Expertise and Qualification 11](#_Toc203031566)

[4.3.7 Logistical Conditions 12](#_Toc203031567)

[4.3.8 Regulatory, Quality and Standards 12](#_Toc203031568)

[4.3.9 Security screening and security clearance requirements 12](#_Toc203031569)

[4.3.10 Confidentiality and non -disclosure conditions 13](#_Toc203031570)

[4.3.11 Guarantee and warranties 14](#_Toc203031571)

[4.3.12 Intellectual Property Rights 14](#_Toc203031572)

[4.3.13 Counter Conditions 15](#_Toc203031573)

[4.3.14 Fronting 15](#_Toc203031574)

[4.3.15 Business Continuity and Disaster Recovery Plans 15](#_Toc203031575)

[4.3.16 Supplier Due Diligence 15](#_Toc203031576)

[4.3.17 Preference Goal Requirements conditions 15](#_Toc203031577)

[3.3.2 Declaration of compliance and acceptance SCC 16](#_Toc203031578)

[4.4 Price and Preference Points Evaluation (Stage 4) 16](#_Toc203031579)

[4.5 Preference Requirements 18](#_Toc203031580)

[Annex A: Bidder substantiating evidence 24](#_Toc203031581)

[5. Technical Mandatory Requirement Evidence 24](#_Toc203031582)

[5.1 Bidder Certification / Affiliation Requirements 24](#_Toc203031583)

[5.2 SITA Certification Requirements 24](#_Toc203031584)

[5.3 Bidder Experience and Capability Requirements 24](#_Toc203031585)

[5.4 Product/Service Hardware Requirements 25](#_Toc203031586)

[5.5 Special Conditions of Contract 25](#_Toc203031587)

[5.6 Preference Points Preferential Goals Evidence 25](#_Toc203031588)

[Annex B: MIOS Certification Requirements/Compliance 27](#_Toc203031589)

# Purpose and Background

* 1. **Purpose**

The purpose of this RFB is to invite Suppliers (hereinafter referred to as “bidders”) to submit bids for the appointment of a service provider for the planning, design, supply, installation and configurations of a total network access control (NAC) solution with maintenance and support for a period of five (5) years.

* 1. **Background**

The procurement of network access control (NAC) solution will ensure a secure and protected network that will allow greater access control in the whole organization (SITA), Improved visibility and accurate device identification.

# Scope of Bid

The scope of work for the bidders is as follows:

1. Install and configuration a multitenant network access control (NAC) platform.

Device/Virtual installation of the solution in a SITA private cloud environment.

1. The platform must have the capability to onboard at least 20 tenants from different VPN and any additional tenants on a time and material basis, as and when required.
2. Maintenance and support for the period of five (5) years.
3. Network access control (NAC) with full functionality features and Licensing.
4. A minimum of 3800 user licenses will be procured for this bid and any additional user licenses on a time and material basis, as and when required.
5. Primary and secondary administration nodes for high availability and to ensure uninterrupted service.
6. The NAC solution must be deployed on a SITA cloud platform.
7. Client based node/thin-client for secondary authentication on-site in case of failure to access the main host.
8. Platform Setup and Configuration:
9. **Infrastructure Provisioning:** Set up the necessary hardware and virtual environments for the NAC platform.
10. **Software Installation:** Install and configure NAC software components, ensuring compatibility with SITA NGN and tenant VPNs.
11. **Multitenancy Configuration:** Configure the platform to support multiple tenants, ensuring data and access segregation.
12. Integration with SITA NGN and VPNs:
    * 1. **Network Integration:** Integrate the NAC platform with the SITA NGN infrastructure (switches, routers, firewalls).
      2. **VPN Integration:** Configure and test VPN connections for each tenant, ensuring secure and reliable access**.**
      3. Integration with existing identity providers (Active Directory, LDAP, RADIUS)
13. Centralized general policy management and enforcement, with ability to configure client-specific rules for granular access control.
14. Role-based access control to manage different levels of user permissions.
15. Endpoint security and compliance checks.
16. Continuous monitoring of connected devices and automated quarantine for non-compliant or unauthorized devices.
17. Support for various authentication methods, including 802.1X for both wired and wireless and must Integrate with various security solutions.
18. Detailed logs of authentication events, access attempts, and policy violations, real-time dashboards for administrators.
19. Documentation of equipment and project which include but not limited to Configuration, Design etc.
20. Training of SITA Technical Staff on new Infrastructure for operational support (non-certification training).
21. Project Management.

# Product / Service Requirements

#### Technical Specification

**NB:** The solution must be deployed on a SITA cloud platform.

Table 1: Technical Specification

|  |  |  |
| --- | --- | --- |
| **Technical Specification** | **Specific Requirements** | |
| **Installation and deployment** | Platform architecture | The product can be deployed on PMs and VMs. It can be deployed in the single-node or cluster mode. Services are not interrupted in the event of any node failure in the cluster. All models support remote DR deployment. If the primary system fails, services are automatically switched to the remote backup system. |
| Cross-domain convergence | The product supports one set of software to centrally manage wired and wireless devices on a single campus network, multi-branch campus networks, and WANs. Wizard-style menus are supported to configure cross-scenario services in an end-to-end manner. |
| Management scale | A single cluster can be smoothly expanded to a multi-cluster system. |
| Licence | Provide at least 10000 authenticated terminal licenses，and support up to 20000 access terminals |
| Tenants | Support multi-tenant authentication, and provide at least a minimum of 20 tenant licenses |
| Deployment Scheme | Turnkey project. Provide cluster deployment, disaster recovery and automatic switchover function |
| **Access authentication** | Data source interconnection | Supports interconnection with multiple identity sources, such as AD/LDAP, WeCom, DingTalk, and Azure AD. Supports synchronization with multiple AD/LDAP domain name servers, local role mapping based on account attributes, and role-based network access authorization. |
| Built-in CA | Supports built-in CA servers to meet enterprises' CA O&M requirements, such as issuing, reporting loss, and handling expiration of personal certificates. The personal certificates can be used as identity sources for network access authentication. |
| Authentication scenario | Supports multi-factor authentication based on multiple identity source combinations, such as account + RADIUS token, password + SMS, TACACS + RADIUS token, and two-factor authentication in SSL VPN mode. |
| Supports multiple authentication technologies, such as 802.1X authentication, MAC address authentication, Portal authentication, VPN authentication, and PPSK/DPSK authentication. Supports PAP, CHAP, EAP-MD5, EAP-PEAP-MSCHAPV2, EAP-TLS, EAP-TTLS-PAP, EAP-PEAP-GTC, and HACA authentication protocols. Allows IPv6 terminals to access the network through 802.1X, MAC address, and Portal authentication. |
| Multiple attributes of the authentication network can be automatically bound upon the first authentication to restrict users' network access behavior. Network attributes include: IP/MAC address of the user authentication device, IMSI and ESN of the SIM or USIM card, and IP address, access VLAN, and access port of the access device |
| Supports 5G networking terminals as well as internal network access rights management through the identity admission system. |
| Supports user-unaware Portal authentication. Supports certificate-based user-unaware authentication. Certificates can be automatically downloaded and installed. |
| Supports TACACS authentication. The user group, account, role, access device group, terminal IP address range, and time range can be used as authentication matching policies. The command set and command template can be used as authorization results. Authentication and authorization logs as well as user login and logout logs can be recorded. |
| Authorization policy | Supports network access policy authorization management based on network attributes such as user/user group/role, location access, device group, access time, access mode, and compliance status. Standard user-defined RADIUS attributes can be used as authorization parameters. Supports priority management for multiple authorization policies. |
| VLAN, ACL, dynamic ACL, security group or VIP user, redirection URL, uplink and downlink bandwidth, and user-defined RADIUS attributes can be used as the network access authorization result. |
|  | Supports self-service guest registration (approval-free or administrator-approved options), or guest access authentication approved by receptionists via mobile terminals. Supports predefined Portal page with built-in languages, such as English. |
| Free mobility | Supports group-based policy management to prevent IP network segment-based ACL specification overload. Supports free mobility in non-VXLAN networking and the separation of authentication points and policy points. Is compatible with devices from multiple vendors. Free mobility can be configured in the RADIUS relay authentication scenario. |
| Online terminal management | Limits the online duration or traffic volume of terminal users. When the online duration or traffic volume reaches the preset thresholds, the users are forced to go offline. The maximum number of access terminals and Portal authentication-free validity period can be limited. |
| Portal authentication users can switch between multiple networks without re-login. |
| **O&M** | Large-screen | Supports display of the network large screen based on the network, application, and user/terminal. The large screen is interactive and configurable. Allows users to drill down to the site topology and device details from the GIS. It also provides full-path display of network faults, user journey, and application quality. |
| Rights- and domain-based management | Allows users to predefine and customize administrator roles, assign system permissions such as management, monitoring, configuration, and maintenance to administrators, and flexibly divide administrators' management scopes by device group, logical network, and access user/terminal group. |
| Agile report | Supports flexible report function definition in multiple dimensions, such as network performance (resource usage, traffic, and link quality), alarms, access authentication, and terminal type statistics. Users can customize the report content, including chart types, data dimensions, and measurement indicators, export reports online, sent them by email at a scheduled time, or display them on the home page. |

## Special Requirements

The planning, design, supply, installation and configurations of a total network access control (NAC) solution with maintenance and support for the period of Five (5) years.

1. Detailed requirements and design documentation.
2. Configured and integrated NAC platform.
3. Defined and implemented access control policies.
4. Testing and validation reports.
5. Training sessions with SITA technical support and comprehensive documentation.
6. Successful deployment and go-live support.
7. Ongoing maintenance and support services.

# Bid Evaluation Stages

The bid evaluation process consists of four stages, according to the nature of the bid. A bidder must qualify for each stage to be eligible to proceed to the next stage of the evaluation. The stages are:

Table 2: Bid Evaluation Stages

|  |  |  |
| --- | --- | --- |
| **Stage** | **Description** | **Applicable for this bid YES/NO** |
| Stage 1 | Mandatory Administrative Responsiveness | YES |
| Stage 2 | Technical Mandatory responsiveness | YES |
| Stage 3 | Special Conditions of Contract verification | YES |
| Stage 4 | Price and Preference Points Evaluation | YES |

## Mandatory Administrative Responsiveness (Stage 1)

### Attendance of briefing session

1. A **non-compulsory virtual briefing session** will be held. The bidder must sign the briefing session attendance register using the same information (bidder company name, bidder representative person name and contact details) as submitted in the bidder’s response document.
2. Bidders need to complete all the SBD documents which needs to be submitted as stated in the Invitation to Bid Document.

### Registered Supplier

1. Only responses from bidders who are registered as a Supplier on National Treasury’s Central Supplier Database (CSD) in terms of National Treasury’s Instruction Note 4A of 2016/17 will be considered for award on this RFB.
2. In the case of joint ventures or consortiums the bidder must demonstrate that at least one of the parties to the bid response attended the briefing session

### Bid Submission Instructions

**Note that a Two Envelope process will be followed and therefore bidders must submit as follows:**

1. **Envelope 1: RFB Document and Technical / Functionality Response**

The following must be included and submitted in a in a separate envelope:

* 1. One (1) original file excluding pricing; **and**
  2. One (1) hard copy excluding pricing; **and**
  3. Two (2) electronic copies on USB memory stick/ flash drive in Portable Document Format (PDF) of the RFB Document and Technical / Functionality Response.

1. **Envelope 2: Price Response**

The following must be included and submitted in a in a separate envelope:

* 1. One (1) original file excluding Technical / Functionality Response; and
  2. One (1) hard copy excluding Technical / Functionality Response; and
  3. Two (2) electronic copies on USB memory stick/ flash drive in Portable Document Format (PDF) of pricing only.

1. It is the Bidder’s responsibility to ensure that the information and contents on the electronic copies is the same as in the hard copies.
2. To ensure that the electronic copies are not damaged, the bidder must submit the USB’s (memory stick/ flash drive) in a sealed padded envelop and be clearly marked.
3. Bidders shall submit proposal responses in accordance with the prescribed manner of submission as specified above. **Failure to comply with the above instructions on submitting a proposal will lead to disqualification.**
4. The **RFB** Responses (hard and electronic copies) must be clearly marked as follows: Bidder’s Name & Contact Details, **RFB** Number, **RFB** Description, and Closing Date.
5. All Bids in this regard shall only be accepted if they have been placed in the tender box before or on the closing date and stipulated time.
6. Late bids shall not be considered.
7. The proposal must be signed by an authorised employee, agent or representative of the bidder. The proposal must bear the initials of the signatory at the bottom of every page as an indication that the bidder has familiarised itself with the terms and conditions of this **RFB** document.
8. Faxed or e-mailed bids will not be accepted.
9. Bidders shall submit proposal responses in accordance with the prescribed manner of submission as specified in this document. **Failure to comply with the bid submission requirements will lead to disqualification.**
10. Bidders are required to submit all returnable documents/information together with their Bids/proposals on or before the closing time and date of the Bids/proposals.
11. All services supplied in accordance with the bidder’s proposal must be in accordance with all applicable legal requirements in terms of South African law, policies and regulations.

## Technical returnable documents

### Instruction and evaluation criteria

1. The bidder must comply with ALL the requirements as per the Technical Mandatory Requirements below by providing substantiating evidence in the form of documentation or information, failing which it will be regarded as “NOT COMPLY”.
2. The bidder must provide a unique reference number (e.g. binder/folio, chapter, section, page) to locate substantiating evidence in the bid response.
3. The bidder must comply with ALL the TECHNICAL MANDATORY REQUIREMENTS in order for the bid response to proceed to the next stage of the evaluation.

### Technical Mandatory Requirements (Stage 2)

Table 3: Technical Mandatory Requirements

| **Mandatory Requirements** | **Substantiating evidence of compliance (used to evaluate bid)** | **Evidence reference (to be completed by bidder)** |
| --- | --- | --- |
| 1. **Bidder Certification/ Affiliation Requirements** | | |
| The bidder **must** be accredited with the Original Equipment Manufacturer (OEM)/Original software Manufacturer (OSM) as a partner/reseller/distributor for the Network Access Solution (NAC). | Attach to **ANNEX A** copy of valid letter from the OEM/OSM as proof that the Bidder is an accredited partner/reseller/distributor for the Network Access Solution (NAC).  **NOTE (1)**  The valid letter clearly indicating the following information below:  (a) The Regulator name (OSM); **and**  (b) The Bidder’s name; **and**  (c) The date it was issued; **and**  (d) if applicable, the expiry date  **NOTE (2):**  SITA reserves the right to verify information provided. | <provide unique reference to locate substantiating evidence in the bid response – **see Annex A, par 5.1**> |
| 1. **SITA Certification Requirements** | | |
| The Bidder must confirm compliance to SITA certification on proposed network access control (NAC) Solution. | The bidder **must** fully complete and submit the MIOS Certification Requirements in **Annex B**. Further to this, the Bidder is required to submit additional information as per below:  a) In the case of a “YES” answer in **Annex B**, the independent certificate(s) to substantiate the declaration.    **Or**  b) In the case of a “N/A” answer in **Annex B**, sufficient motivation as to why the standard is not deemed applicable.  **NOTE (1):**  An empty declaration (no answer provided), or a "N/A" answer without sufficient motivation, will be regarded as a “NO” answer, and will be considered as non-compliant.  **NOTE (2):**  SITA reserves the right to verify the information provided. | <provide unique reference to locate substantiating evidence in the bid response – see **Annex A, par 5.2, Annex B>** |
| 1. **Bidder Experience and Capability Requirements** | | |
| The bidder **must** have supplied, planned, designed, installed and configured network access control (NAC) solution to at least one (1) customer within the last five (5) years from publication date of this bid. | The bidder must provide reference details from at least one (1) customer to whom a network access control (NAC) solution was planned, designed, installed and configured within the last five (5) years from publication date of this bid.  **NOTE (1):**  The Bidder **must provide all** of the following information when completing **Table 7:**   1. Company name; and 2. Contact person, telephone **and/or** e-mail address; **and** 3. Project scope of Work; **and** 4. Project start and End date.   **NOTE (2):**  SITA reserves the right to verify information provided.  **NOTE (3):**  Failure to complete Table 7 fully as indicated above will result in disqualification,    **NOTE (4):**  No reference letters required. | <provide unique reference to locate substantiating evidence in the bid response – **see Annex A, par 5.3, Table 7**> |
| 1. **Product/Service Requirements** | | |
| The bidder must confirm compliance to the product/service specification requirements as stated on 2.1.1 Technical Specification. | The bidder must confirm that they comply with the **product/service specification requirements** by providing substantiating evidence in the bid response in a form of a **Brochure/Hardware Specification** of the product capabilities.  **Note (1):**  SITA reserves the right to verify information provided as Brochure/Technical Specification of the product capabilities if they meet technical requirements specification. Failure to meet technical specification will result in disqualification.  **Note (2):**  Failure to provide unique reference to locate substantiating evidence in the bid response in a form of a brochure/Technical Specification of the proposed product capabilities will result in disqualification. | <provide unique reference to locate substantiating evidence in the bid response in a form of a Brochure/Technical Specification of the product capabilities and by completing section **see Annex A, par 5.4.** |
| 1. **Special Condition of Contract** | | |
| Bidder must accept ALL the Special Conditions of contract. | The Bidder must accept ALL the Special Conditions of Contract by completing and signing the declaration of Acceptance in the Declaration of Compliance and Acceptance under the Special Conditions (**Section 4.3.2**).  **NOTE (1):**  Failure to accept ALL the Special Conditions of Contract will result in disqualification. | <Provide unique reference to locate substantiating evidence in the bid response – see **Annex A, par 5.5**> |

## Special Conditions of Contract Verification (Stage 3)

1. The successful supplier will be bound by Government Procurement: General Conditions of Contract (GCC) as well as this Special Conditions of Contract (SCC), which will form part of the signed contract with the successful Supplier. However, SITA reserves the right to include or waive the condition in the signed contract.
2. SITA reserves the right to:
   1. Negotiate the conditions; or
   2. Automatically disqualify a bidder for not accepting these conditions; or
   3. Award to multiple bidders
   4. Not to award; or
   5. To do a partial award
3. In the event that the bidder qualifies the proposal with own conditions and does not specifically withdraw such own conditions when called upon to do so, SITA will invoke the rights reserved in accordance with subsection 4.3. (b) Above.

### Special Conditions of Contract

### 4.3.1.1 Contracting Conditions

1. **Formal Contract** - The supplier must enter into a formal written contract (agreement) with SITA.
2. **Right to Audit** - SITA reserves the right, before entering into a contract, to conduct or commission an external service provider to conduct a financial audit or probity to ascertain whether a qualifying bidder has the financial wherewithal or technical capability to provide the goods and services as required by this tender.

### 4.3.1.2 Delivery Address

1. The supplier must deliver the required products or services at 459 John Vorster Dr, Centurion, Pretoria, 0048 SITA offices.

### 4.3.1.3 Services and Performance Metrics

1. The bidder is responsible to provide the following services as specified in the Service Breakdown Structure (SBS):
   1. **Operational MTTResolve: Response and Repair Times -** The Bidder must perform corrective maintenance within predefined response and repair times. Maximum Time To Repair in all cases (Full Service Agreement) will be sixteen (16) working hours for all incidents.
   2. **Mission Critical MTTResolve: Response and Repair Times** - The Bidder must perform corrective maintenance within predefined response and repair times. Maximum Time To Repair in all mission critical cases (Full Service Agreement) will be one (1) working hour incidents.

### 4.3.1.4 Supplier Performance Reporting

The supplier reporting will be detailed in the service level agreement (SLA) with the provided successful bidder.

### 4.3.1.5 Certification, Expertise and Qualification

1. The bidder certifies that:
   1. it has the necessary expertise, skill, qualifications and ability to undertake the work required in terms of the Statement of Work or Service Definition
   2. it is committed to provide the Products or Services; and
   3. perform all obligations detailed herein without any interruption to the Customer
   4. it has been certified for the Products and Services required

### 4.3.1.6 Logistical Conditions

1. **Hours of Work**
   1. Office hours are defined as business working hours of the customer and is Mondays to Fridays between 07:30 and 16:00.
   2. After hours of the customer during weekdays are from16:00 to 07:30.
   3. All mission critical sites will be managed on 24 x 7 x 365 days a year including public holidays.
2. **Client environment**
   1. In the event that SITA grants the bidder access to Environment including hardware, software, internet facilities, data, telecommunication facilities and/or network facilities remotely, the Supplier must adhere to SITA's relevant policies and procedures (which policy and procedures are available to the Supplier on request) or in the absence of such policy and procedures, in terms of, best industry practice.
3. **Tools of Trade**
   1. The bidder is expected to use its own resources (cell phone, laptops etc) to communicate with its own offices or outside of the SITA/Client buildings, including all tools and equipment to render the services effectively.
4. **Remedy ARS Support**
   1. Information systems

### 4.3.1.7 Regulatory, Quality and Standards

1. The Supplier must for the duration of the contract ensure compliance with Protection of Personal Information Act, 2013 (POPIA).

### 4.3.1.8 Security screening and security clearance requirements

* 1. **Company security screening**: The supplier may be required to undergo a company security screening conducted by the State Security Agency (SSA). Should the SSA find the supplier not suitable after the conduct of the security screening, the business relationship will be terminated. The following documentation will be required for the company security screening process to be conducted:
     1. Copy of company registration documentation.
     2. Copy(ies) of identity documentation of Director(s), Member(s) or Trustee(s);
     3. Copy of valid tax clearance certificate.
  2. **Security suitability check for individuals:** SITA may, at its own discretion and in line with its policies and procedures, require employees of the supplier to be subjected to a security suitability check before commencement of a project or delivering of a service. The security suitability check is conducted by SITA in order to ensure that individuals meet the minimum-security requirements and also to verify personal information. The supplier will be required to replace any employee(s) who is found to be not suitable after the conduct of the security screening. The following documentation will be required for the security suitability check:
     1. Copy of identity document;
     2. Copy(ies) of qualification(s) if SITA requires verification thereof;
     3. Fingerprints – will be taken electronically;
     4. Signed consent form for the conduct of background checks.
  3. **Security clearance:** A security clearance, issued by either the SSA or Defence Intelligence (DI) is required if any employee of the supplier will have or may gain access to classified information throughout the duration of the project or in the process of delivering a service. The level of security clearance required – Confidential, Secret or Top Secret, will be determined at the sole discretion of SITA. The supplier will have to replace any employee who do not qualify for a security clearance or is found not suitable by the SSA or DI. The following documentation will be required for the security clearance process:
     1. Completed Z204 or DD1057 security clearance application form;
     2. Fingerprints;
     3. Personal documentation of the applicant, including but not limited to, identity document, passport, marriage certificate (if applicable), divorce order (if applicable), qualifications, salary advice and bank statements.

### 4.3.1.9 Confidentiality and non -disclosure conditions

1. The Supplier, including its management and staff, must before commencement of the Contract, sign a non-disclosure agreement regarding Confidential Information
2. Confidential Information means any information or data, irrespective of the form or medium in which it may be stored, which is not in the public domain and which becomes available or accessible to a Party as a consequence of this Contract, including information or data which is prohibited from disclosure by virtue of:
   1. the Promotion of Access to Information Act, 2000 (Act no. 2 of 2000);
   2. being clearly marked "Confidential" and which is provided by one Party to another Party in terms of this Contract;
   3. being information or data, which one Party provides to another Party or to which a Party has access because of Services provided in terms of this Contract and in which a Party would have a reasonable expectation of confidentiality;
   4. being information provided by one Party to another Party in the course of contractual or other negotiations, which could reasonably be expected to prejudice the right of the non-disclosing Party;
   5. being information, the disclosure of which could reasonably be expected to endanger a life or physical security of a person;
   6. being technical, scientific, commercial, financial and market-related information, know-how and trade secrets of a Party;
   7. being financial, commercial, scientific or technical information, other than trade secrets, of a Party, the disclosure of which would be likely to cause harm to the commercial or financial interests of a non-disclosing Party; and
   8. being information supplied by a Party in confidence, the disclosure of which could reasonably be expected either to put the Party at a disadvantage in contractual or other negotiations or to prejudice the Party in commercial competition; or
   9. information the disclosure of which would be likely to prejudice or impair the safety and security of a building, structure or system, including, but not limited to, a computer or communication system; a means of transport; or any other property; or a person; methods, systems, plans or procedures for the protection of an individual in accordance with a witness protection scheme; the safety of the public or any part of the public; or the security of property; information the disclosure of which could reasonably be expected to cause prejudice to the defence of the Republic; security of the Republic; or international relations of the Republic; or plans, designs, drawings, functional and technical requirements and specifications of a Party, but must not include information which has been made automatically available, in terms of the Promotion of Access to Information Act, 2000; and information which a Party has a statutory or common law duty to disclose or in respect of which there is no reasonable expectation of privacy or confidentiality;
3. Notwithstanding the provisions of this Contract, no Party is entitled to disclose Confidential Information, except where required to do so in terms of a law, without the prior written consent of any other Party having an interest in the disclosure;
4. Where a Party discloses Confidential Information which materially damages or could materially damage another Party, the disclosing Party must submit all facts related to the disclosure in writing to the other Party, who must submit information related to such actual or potential material damage to be resolved as a dispute;
5. Parties may not, except to the extent that a Party is legally required to make a public statement, make any public statement or issue a press release which could affect another Party, without first submitting a written copy of the proposed public statement or press release to the other Party and obtaining the other Party's prior written approval for such public statement or press release, which consent must not unreasonably be withheld.

### 4.3.1.10 Guarantee and warranties

1. The supplier confirms that:
   1. The warranty of goods supplied under this contract remains valid for the duration of the contract after the goods were delivered, installed and commissioned with a sign off, including the client’s signature
   2. as at Commencement Date, it has the rights, title and interest in and to the Product or Services to deliver such Product or Services in terms of the Contract and that such rights are free from any encumbrances whatsoever;
   3. the Product is in good working order, free from Defects in material and workmanship, and substantially conforms to the Specifications, for the duration of the Warranty period;

### 4.3.1.11 Intellectual Property Rights

1. SITA retains all Intellectual Property Rights in and to SITA's Intellectual Property. As of the Effective Date, the Supplier is granted a non-exclusive license, for the continued duration of this Contract, to perform any lawful act including the right to use, copy, maintain, modify, enhance and create derivative works of SITA's Intellectual Property for the sole purpose of providing the Products or Services to SITA pursuant to this Contract; provided that the Supplier must not be permitted to use SITA's Intellectual Property for the benefit of any entities other than SITA without the written consent of SITA, which consent may be withheld in SITA's sole and absolute discretion. Except as otherwise requested or approved by SITA, which approval is in SITA's sole and absolute discretion, the Supplier must cease all use of SITA's Intellectual Property, at of the earliest of:
   1. termination or expiration date of this Contract;
   2. the date of completion of the Services; and
   3. the date of rendering of the last of the Deliverables
2. If so required by SITA, the Supplier must certify in writing to SITA that it has either returned all SITA Intellectual Property to SITA or destroyed or deleted all other SITA Intellectual Property in its possession or under its control
3. SITA, at all times, owns all Intellectual Property Rights in and to all Bespoke Intellectual Property.
4. Save for the license granted in terms of this Contract, the Supplier retains all Intellectual Property Rights in and to the Supplier’s pre-existing Intellectual Property that is used or supplied in connection with the Products or Services
5. Provide SITA with the compliant Occupational Health and Safety File (required on site for period of installation and proof of compliance).

### 4.3.1.12 Counter Conditions

1. Bidders’ attention is drawn to the fact that amendments to any of the Bid Conditions or setting of counter conditions by bidders may result in the invalidation of such bids.

### 4.3.1.13 Fronting

1. The SITA supports the spirit of Broad Based Black Economic Empowerment and recognizes that real empowerment can only be achieved through individuals and businesses conducting themselves in accordance with the Constitution and in an honest, fair, equitable, transparent and legally compliant manner. Against this background the SITA will not condone any form of fronting.
2. The SITA, in ensuring that bidders conduct themselves in an honest manner will, as part of the bid evaluation processes, conduct or initiate the necessary enquiries/investigations to determine the accuracy of the representation made in bid documents. Should any of the fronting indicators as contained in the Guidelines on Complex Structures and Transactions and Fronting, issued by the Department of Trade and Industry, be established during such enquiry/investigation, the onus will be on the bidder / contractor to prove that fronting does not exist. Failure to do so within a period of 14 days from date of notification may invalidate the bid / contract and may also result in the restriction of the bidder/contractor to conduct business with the public sector for a period not exceeding ten (10) years, in addition to any other remedies SITA may have against the bidder/contractor concerned.

### 4.3.1.14 Business Continuity and Disaster Recovery Plans

1. The bidder confirms that they have written business continuity and disaster recovery plans that define the roles, responsibilities and procedures necessary to ensure that the required services under this bid specification is in place and will be maintained continuously in the event of a disruption to the bidder’s operations, regardless of the cause of the disruption.

### 4.3.1.15 Supplier Due Diligence

1. SITA reserves the right to conduct supplier due diligence prior to final award or at any time during the Contract period and this may include pre-announced / non-announced site visits. During the due diligence process the information submitted by the bidder will be verified and any misrepresentation thereof may disqualify the bid or Contract in whole or parts thereof.

### 4.3.1.16 Preference Goal Requirements conditions

1. The Bidder’s commitment for the Preference Goal Requirements in this tender will be legally binding and the Bidder needs to perform against their commitment for the duration of the contract which will form part of the Contractual Agreement.
2. The Bidder must sustain, or improve the company’s BBBEE Level for the duration of the contact which will form part of the Contractual Agreement.
3. Performance of Preference Goal Requirements will be determined annually. Bidders must submit their Preference status report indicating progress against the Bidder’s preferential commitments within 30 days of the yearly anniversary of the contract.
4. Bidders need to keep auditable substantive records / evidence and upon request by SITA must be made available for audit and, or due diligence purposes.
5. SITA reserves the right to require from a Bidder, either before a bid is adjudicated or at any time subsequently, to substantiate any claim with regards to preferences, in any manner required by SITA.
6. SITA reserves the right to verify information / evidence provided by the Bidder.
7. SITA reserves the right to introduce a **penalty of 1%** of the overall annual year spent by SITA for the prior year if the Bidder fails to comply to **paragraphs (a), (b) and (c) above**.

### 4.3.2 Declaration of compliance and acceptance SCC

I (we), the bidder hereby declares that I (we) accept ALL the Special Conditions of Contract as specified in par 4.3.1 above and shall comply with all stated obligations:

Name of Bidder: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

## Price and Preference Points Evaluation (Stage 4)

* + 1. **Costing and preference evaluation**

1. In terms of the SITA Preferential Procurement Policy (PPP), the following preference point system is applicable to all Bids:
   1. the 80/20 system (80 Price, 20 Specific Goals) for requirements with a Rand value of up to R50 000 000 (all applicable taxes included); or
2. The Applicable Preference Point system for this tender is the **80/20** preference point system.
3. Points for this tender shall be awarded for:
   1. Price; and
   2. Preference points for specific goals.
4. The maximum points for this tender will be allocated as follows, subject to par.2.

**Table 4: Points Allocation**

|  |  |
| --- | --- |
| **Description** | **Points** |
| Price | **80** |
| Preference points for specific goals | **20** |
| Total points for Price and preference points for specific goals | 100 |

* + 1. **Costing and Pricing Conditions**
    2. **South African Pricing** –

The total price must be VAT inclusive and be quoted in South African Rand (ZAR).

* + 1. **Total Price**

Bidder will be bound by the following general costing and pricing conditions and SITA reserves the right to negotiate the conditions or automatically disqualify the bidder for not accepting these conditions:

* 1. All quoted prices are the total price for the entire scope of required services and deliverables to be provided by the bidder.
  2. All additional costs as well as cost of delivery, labour, S&T, overtime, etc. must be included in this bid.
  3. All services, accessories, upgrades and options required by the solution or specified by the client must be included in the quoted price. If not included, suppliers will be required to supply these accessories at no cost to the client.
  4. SITA reserves the right to negotiate pricing with the successful bidder prior to the award as well as envisaged quantities

2.1. These conditions will form part of the Contract between SITA and the bidder. However, SITA reserves the right to include or waive the condition in the Contract.

2.2. The bidder must complete the declaration of acceptance as per **par 5** below by marking with an “X” either “ACCEPT ALL”, or “DO NOT ACCEPT ALL”, failing which the declaration will be regarded as “DO NOT ACCEPT ALL” and the bid will be disqualified.

* + 1. **Rate of Exchange Pricing Information**

Provide the TOTAL BID PRICE for the duration of Contract and clearly indicate the Local Price and Foreign Price, where –

1. **Local Price** means the portion of the TOTAL price that is NOT dependent on the Foreign Rate of Exchange (ROE) and;
2. **Foreign Price** means the portion of the TOTAL price that is dependent on the Foreign Rate of Exchange (ROE).
3. **Exchange Rate** means the ROE (ZA Rand vs foreign currency) as determined at time of bid.
   * 1. **Bid Exchange Rate Conditions**

The bidders must use the exchange rate provided below to enable SITA to compare the prices provided by using the same exchange rate:

|  |  |
| --- | --- |
| **Foreign currency** | **South African Rand (ZAR) exchange rate** |
| 1 US Dollar | **R17.99** |
| 1 Euro | **R20.77** |
| 1 Pound | **R23.91** |

**Note (1):**

The ROE indicated above is to ensure a competitive bidding process.

**Note (2):**

The ROE will be fluctuating. The details of the ROE fluctuation will be negotiated during the contracting stage

* + 1. **Bid Pricing Schedule**

Bidders **must** complete the bid pricing schedule in the Excel spreadsheet format provided and upload this as part of their submission.

**NOTE:**

Bidders must complete and submit bid pricing in the provided Excel spreadsheet format, and any pricing schedule submitted in a different format will not be considered.

* + 1. **Declaration of Acceptance**

|  | **ACCEPT ALL** | **DO NOT ACCEPT ALL** |
| --- | --- | --- |
| 1. The bidder declares to ACCEPT ALL the Costing and Pricing conditions as specified in **par 4.4.2** above by indicating with an “X” in the “ACCEPT ALL” column, or 2. The bidder declares to NOT ACCEPT ALL the Costing and Pricing Conditions as specified in **par 4.4.2** above by -    1. Indicating with an “X” in the “DO NOT ACCEPT ALL” column, and;    2. Provide reason and proposal for each of the condition not accepted. |  |  |
| **Comments by bidder:**  Provide the condition reference, the reasons for not accepting the condition. | | |

## Preference Requirements

1. **The bidder must complete in full all the PREFERENCE requirements.**
2. **Allocation of points per requirements:** The point’s allocation of bidders’ responses to the requirements will be determined by the completeness, relevance and accuracy of substantiating evidence.
3. Points will be allocated for each **PREFERENCE requirement** as per the criteria set in each section in the **table 7** below.
4. **The bidder must provide a unique reference number** (e.g. binder/folio, chapter, section, page) to locate substantiating evidence in the bid response. During evaluation, SITA reserves the right to treat substantiation evidence that cannot be located in the bid response, as “NOT COMPLY”. The evidence needs to be attached to **ANNEX A**.
5. **Preference Goal Requirements:**
   1. The applicable Preference Point system for this tender and points claimed is **80/20.**
   2. The specific Preferential Goal Requirements for this tender is indicated in **table 6** below.
   3. The Bidder must complete 80/20 preference point system and submit proof or documentation required in terms of this tender.
   4. The Bidder **must indicate their commitment** to claim points for each of the preference points by signing at par 4.5 in the Invitation to Bid document.
   5. Failure on the part of a bidder to submit proof or documentation required or to comply to **paragraph (d)** above in terms of this tender to claim preference points for the **Preference Goal Requirements** for this tender, will be interpreted to mean that preference points are not claimed.
   6. The Bidder’s **commitment** for the **Preference Goal Requirements** in this tender will be **legally binding** and the Bidder needs to **perform against their commitment** for the duration of the contract which will form part of the Contractual Agreement.
   7. The Bidder **must sustain, or improve** the company’s BBBEE Level for the duration of the contact which will form part of the Contractual Agreement.
   8. **Performance of Preference Goal Requirements will be determined annually.** Bidders must submit their Preference status report to SITA indicating progress against the Bidder’s preferential commitments **within 30 days after each quarter from the commencement date of the contract**.
   9. Bidders need to keep auditable substantive records / evidence and upon request by **SITA** must be made available for audit and, or due diligence purposes.
   10. **SITA reserves the right** **to** require from a Bidder, either before a bid is adjudicated or at any time subsequently, to substantiate any claim with regards to preferences, in any manner required by SITA.
   11. **SITA reserves the right to** verify information / evidence provided by the Bidder.
   12. **SITA reserves the right to** introduce a **penalty of 1%** of the overall annual year spent by **SITA** for the prior year if the Bidder fails to comply with **paragraphs (f), (g) and (h) above.**

**Table 5:** Preference Goal Requirements

| **Preference Goal Requirement #** | **Preferential Goal Requirements** | **Preferential Goal Requirements** | |
| --- | --- | --- | --- |
|  | **Preferential Goal Requirements allocated for this tender** | **Substantiating evidence and evidence reference to be completed by bidder.  Evaluation per requirement: Each requirement indicated in the table below must be completed and points will be allocated based on the evidence required below**  **Evidence Reference** | |
|  | **B-BBEE Requirements** |  | |
| 1) | **B-BBEE Requirements**  Promotion of Transformational Objectives. | **Evidence:** The Bidder must provide a copy of the following relevant evidence for the Preferential Goal points which the Bidder qualifies for:   1. **Columns A, B, C and D in table 6**   Copy of relevant proof ***(B-BBEE certificate or sworn affidavit)*** of B-BBEE status level of contributor as defined in the Broad-Based Black Economic Empowerment Act:   * + - * 1. ***B-BBEE certificate*** *(from a SANAS Accredited Agency);*   **or**   * 1. ***Sworn affidavit*** in the format provided by CIPC - ***Applicable to EMEs and QSEs only;***   **and/ or**   1. **Column D in tables 6**   Copy of ***South African Identification Document (ID***);  **and/ or**   1. **Column E in tables 6**   *Copy of Medical Certificate* ***clearly indicating the disability in line with the B-BBEE status claimed as defined in the Broad-Based Black Economic Empowerment Act***.  **Note:**  The CIPC (Companies and Intellectual Property Commission) registration documents will also be used as evidence to confirm compliance to the Preferential procurement requirements as part of the evaluation process.  **Points allocation:** Points will be allocated for bidders that meets the requirements as indicated in either **table 6 in section 4.5.1.** | <provide unique reference to locate the substantiating evidence in the bid response – **Annex A, section 5.6**> |

**Table 6**: **B-BBEE Points as part of the Preference Goal requirements (Preferential Goal Requirements for (80/20) system)**

**Note: Bidder to select the section for points they wish to claim (Mark as Y=Yes) in the table below.**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  | **Ownership** | | | |  |  |  |
|  | **Reference #** | **Contributor Level as defined in the Broad-Based Black Economic Empowerment Act** | **EME/QSEs** | **Black Owned (BO) (51% or more)** | **Black Woman Owned (BWO) (More than 30%)** | **Youth Owned** | **Owned by People living with disabilities** | **Score** | **Bidder to select the section for points they wish to claim (Mark as Y= Yes)** |  |
|  |  |
|  |  |  | **(A)** | **(B)** | **(C)** | **(D)** | **(E)** | **(F)** |  |  |
|  | **1** | **Level 1** | **6** | **4** | **4** | **4** | **2** | **20** |  |  |
|  | **2** | **Level 1** | **6** | **4** | **2** | **2** | 0 | **14** |  |  |
|  | **3** | **Level 1** | **6** | **4** | **2** | 0 | 0 | **12** |  |  |
|  | **4** | **Level 1** | **6** | **4** | 0 | 0 | 0 | **10** |  |  |
|  | **5** | **Level 2 and 3** | **4** | **2** | **1** | **1** | **1** | **9** |  |  |
|  | **6** | **Level 2 and 3** | **4** | **2** | **1** | **1** | 0 | **8** |  |  |
|  | **7** | **Level 2 and 3** | **4** | **2** | **1** | 0 | 0 | **7** |  |  |
|  | **8** | **Level 2 and 3** | **4** | **2** | 0 | 0 | 0 | **6** |  |  |
|  | **9** | **Level 4 and 5** | **2** | **1** | **0,5** | **0,5** | **0,5** | **4,5** |  |  |
|  | **10** | **Level 4 and 5** | **2** | **0,5** | **0,5** | **0,5** | 0 | **3,5** |  |  |
|  | **11** | **Level 4 and 5** | **2** | **0,5** | **0,5** | 0 | 0 | **3** |  |  |
|  | **12** | **Level 4 and 5** | **2** | **0,5** | 0 | 0 | 0 | **2,5** |  |  |
|  | **13** | **Level 6** | 0 |  | 0 | 0 | 0 | **0** |  |  |
|  | **14** | **Level 7** | 0 |  | 0 | 0 | 0 | **0** |  |  |
|  | **15** | **Level 8** | 0 |  | 0 | 0 | 0 | **0** |  |  |
|  | **16** | **Non-Contributor** | 0 |  | 0 | 0 | 0 | **0** |  |  |
|  | **Total Maximum Score Allocation:** | | **20** |  |  |  |  |  |  |  |

F= A+B+C+D+E

1. Bidder substantiating evidence

# Technical Mandatory Requirement Evidence

## Bidder Certification / Affiliation Requirements

Attach a copy of a valid letter from the OEM/OSM as proof that the bidder is an accredited partner/reseller/distributor for the network access solution (NAC) **here**.

**NOTE (1)**

The valid letter clearly indicating the following information below:

(a) The Regulator name (OSM); **and**

(b) The Bidder’s name; **and**

(c) The date it was issued; **and**

(d) if applicable, the expiry date

**NOTE (2):**

SITA reserves the right to verify information provided.

## SITA Certification Requirements

The bidder must fully complete and submit the MIOS Certification Requirements in **Annex B.** Further to this, the Bidder is required to submit additional information as per below:

a) In the case of a “YES” answer in **Annex B**, the independent certificate(s) to substantiate the declaration.

**Or**

b) In the case of a “N/A” answer in **Annex B**, sufficient motivation as to why the standard is not deemed applicable.

**NOTE (1):**

An empty declaration (no answer provided), or a "N/A" answer without sufficient motivation, will be regarded as a “NO” answer, and will be considered as non-compliant.

**NOTE (2):**

SITA reserves the right to verify the information provided.

## Bidder Experience and Capability Requirements

The bidder must provide reference details from at least one (1) customer to whom a network access control (NAC) solution was planned, designed, installed and configured within the last five (5) years from publication date of this bid.

**NOTE (1)**

The Bidder **must provide all** of the following information when completing **Table 7:**

1. Company name; and
2. Reference Person Name, Tel and / or email; and
3. Project Scope of Work; and
4. Project Start and End date,
5. Scope of work must be related

**NOTE (2):**

Failure to comply fully to the requirements as indicated below in table 7 will result in disqualification.

**NOTE (3):**

SITA reserves the right to verify information provided.

**NOTE (4):**

No reference letters required.

Table 7: References

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No** | **Company Name** | **Reference person name, contact details** | **Project Scope of Work** | **Project start and end date** |
| 1 | <Company name> | <Person Name>  <Tel>  <email> | <Provide scope details of a project from a customer to whom network access control (NAC) solution was planned, designed, installed and configured> | Start Date:  End Date: |

## Product/Service Hardware Requirements

The bidder must confirm that they comply with the product/service specification requirements by providing substantiating evidence in the bid response in a form of a Brochure/Hardware Specification of the product capabilities and attaching **here**.

**NOTE (1):**

SITA reserves the right to verify information provided as Brochure/Technical Specification of the product capabilities if they meet hardware requirements specification. Failure to meet hardware specification will result in disqualification.

**NOTE (2):**

Failure to provide unique reference to locate substantiating evidence in the bid response in a form of a brochure/Technical Specification of the product capabilities will result in disqualification.

## Special Conditions of Contract

The Bidder must accept ALL the Special Conditions of Contract by completing and signing the declaration of Acceptance in the Declaration of Compliance and Acceptance under the Special Conditions (Section 4.3.2).

**NOTE (1):**

**Failure to accept ALL the Special Conditions of Contract will result in disqualification.**

## Preference Points Preferential Goals Evidence

The Bidder must provide a copy of the following relevant evidence for the Preferential Goal points which the Bidder qualifies for:

1. **Columns A, B, C and D in table 6**

Copy of relevant proof ***(B-BBEE certificate or sworn affidavit)*** of B-BBEE status level of contributor as defined in the Broad-Based Black Economic Empowerment Act:

* + - * 1. ***B-BBEE certificate*** *(from a SANAS Accredited Agency);*

**or**

* 1. ***Sworn affidavit*** in the format provided by CIPC - ***Applicable to EMEs and QSEs only;***

**and/ or**

1. **Column D in tables 6**

Copy of ***South African Identification Document (ID***);

**and/ or**

1. **Column E in tables 6**

*Copy of Medical Certificate* ***clearly indicating the disability in line with the B-BBEE status claimed as defined in the Broad-Based Black Economic Empowerment Act***.

**Note:**

The CIPC (Companies and Intellectual Property Commission) registration documents will also be used as evidence to confirm compliance to the Preferential procurement requirements as part of the evaluation process.

**Points allocation:** Points will be allocated for bidders that meets the requirements as indicated in either **table 6 in section 4.5.1.**

1. MIOS Certification Requirements/Compliance

**Regulatory, Quality and Standards**

1. In terms of the State Information Technology Agency Act (as amended), the Agency (SITA) must certify that all ICT goods and services comply with approved interoperability (MIOS 6) and related security standards. These standards are available on the SITA website (http://www.sita.co.za under procurement | Standards menu selection).
2. In accordance with the SITA Act and applicable regulations, SITA hereby declares that the relevant approved standards are applicable.
3. The set of interoperability standards are extracted from MIOS and listed in the table below, are applicable to this tender/request and will be subject to the SITA Certification process. The bidder is required to ensure the following:
4. Declare, by a "YES", "NO", or "N/A" (Not Applicable) answer, the level of compliance with each standard as listed in the table; and
5. In the case of a YES answer, attach, if any, the independent certificate(s) to substantiate the declaration; and in the case of a N/A answer, provide sufficient motivation as to why the standard is not deemed applicable.
6. An empty declaration (no answer provided), or a "N/A" answer without sufficient motivation, will be regarded as a "NO" answer, and could be considered as non-compliant.
7. SITA Certification will assess the level of compliance and issue a certificate to that effect. Non-compliance to any of the listed standards will be regarded as NOT meeting the relevant requirements of the bid.
8. This list is only valid for the latest approved request documentation as received and held by the SITA Certification unit.
9. This list does NOT constitute a Compliance Certificate and ONLY indicates the relevant standards applicable to the system/solution.
10. Once implementation of the awarded solution is complete, please contact the ICT Certification unit at certification@sita.co.za to complete the ICT Certification process.

**Interoperability Standard:**

|  |  |  |
| --- | --- | --- |
| **The solution must comply with the following minimum interoperability standards:** | | **Indicate YES/NO/NOT APPLICABLE (N/A)** |
| C020101 Hypertext Transfer Protocol (HTTP/1.1) | RFC 7230 |  |
| C020102 Hypertext Transfer Protocol (HTTP/1.1) | RFC 7231 |  |
| C020103 Hypertext Transfer Protocol (HTTP/1.1) | RFC 7232 |  |
| C020104 Hypertext Transfer Protocol (HTTP/1.1) | RFC 7233 |  |
| C020105 Hypertext Transfer Protocol (HTTP/1.1) | RFC 7234 |  |
| C020106 Hypertext Transfer Protocol (HTTP/1.1) | RFC 7235 |  |
| C020107 Hypertext Transfer Protocol (HTTP/1.1) | RFC 7236 |  |
| C020108 Hypertext Transfer Protocol (HTTP/1.1) | RFC 7237 |  |
| C020109 Upgrading to TLS within HTTP/1.1 (HTTPS) | RFC 2817 |  |
| C020502 Lightweight Directory Access Protocol (LDAP) | RFC 4510 |  |
| C020503 Lightweight Directory Access Protocol (LDAP) | RFC 4511 |  |
| C020504 Lightweight Directory Access Protocol (LDAP) | RFC 4512 |  |
| C020505 Lightweight Directory Access Protocol (LDAP) | RFC 4513 |  |
| C020506 Lightweight Directory Access Protocol (LDAP) | RFC 4514 |  |
| C020507 Lightweight Directory Access Protocol (LDAP) | RFC 4515 |  |
| C020508 Lightweight Directory Access Protocol (LDAP) | RFC 4516 |  |
| C020509 Lightweight Directory Access Protocol (LDAP) | RFC 4517 |  |
| C020510 Lightweight Directory Access Protocol (LDAP) | RFC 4518 |  |
| C020511 Lightweight Directory Access Protocol (LDAP) | RFC 4519 |  |
| C020802 Internet Protocol v6 (IPv6) | RFC 2460 |  |
| C080301 The Short Message Service Specifications for Mobile Stations | ETS 300 536 |  |
| C080304 The Short Message Service Specifications for Mobile Stations | ETS 300 560 |  |

I, the bidder (Full names) …………………………………………………………. representing (company name) …………………………………………………………….. Hereby confirm that the information as completed is accurate and understand that it will form part of the contract and is legally binding.

Thus done and signed at …………………………………….. On this………day of……………..….20….……………………………….