

**TERMS OF REFERENCE:
FOR
APPOINTMENT OF A SERVICE PROVIDER FOR THE SECURE SOCKETS LAYER (SSL) CERTIFICATE FOR THIRTY-SIX (36) MONTHS**

1. PURPOSE

The purpose of this document is to outline the technical and service requirements for the renewal of the Secure Sockets Layer (SSL) certificate for our systems. This renewal is necessary to restore secure, encrypted communication between our platform and its users, and to ensure compliance with current security standards and best practices.

2. SCOPE OF WORK

The appointed service provider will be required to:

- Assess the current system, environment, and SSL requirements
- Recommend the most appropriate SSL certificate type (e.g., single domain, wildcard, or multi-domain)
- Supply and renew the SSL certificate for the relevant domain(s)
- Perform installation and configuration of the SSL certificate on the designated servers
- Ensure compatibility with all relevant systems, applications, and browsers
- Conduct testing to confirm proper implementation and functionality
- Provide documentation related to the certificate and installation process.

SSL CERTIFICATE RENEWAL FOR THIRTY-SIX (36) MONTHS

3. SCOPE OF SERVICES REQUIRED:

The renewal should cover the following:

- A valid SSL certificate issued by a recognized Certificate Authority (CA)
- Encryption level compliant with current industry standards (e.g., minimum 2048-bit key or higher)
- Warranty and validation levels appropriate to the organization's needs (e.g., Domain Validation, Organization Validation, or Extended Validation)
- Technical support during installation and for the duration of the certificate validity period
- Renewal reminders and Support for future renewals
- Optional: Managed SSL services, including monitoring and automatic renewal (if available).

4. TECHNICAL EVALUATION AND COMPLIANCE WITH SPECIFICATION

The service provider must comply with the following mandatory requirements:

Item	Criteria	Weight
1.	1.1 Company Experience The bidder must provide references where similar work was done. The service provider must have dealt with various organisations, from large to small-scale employees. At least 3 contactable government entities or agencies references where similar services were rendered in the past 3 years. No reference letters – 0 points 2 contactable references – 20 points More than 2 contactable references – 50 points	50

SSL CERTIFICATE RENEWAL FOR THIRTY-SIX (36) MONTHS

2.	Reseller / Authorized Distributor of A CA Bidder must be an authorized reseller or partner of a recognized and trusted Certificate Authority (CA) and must supply SSL certificates issued by such authorities. Official authorized partner/reseller with valid certificate/partnership proof submitted – 10 points Demonstrated reseller relationship with a recognized CA, but limited or indirect proof – 5 points No evidence of ability to supply certificates from a trusted CA – 0 points	15
3.	Proforma Service Level Agreement Bidders must submit a proforma Service Level Agreement (SLA) outlining support services, response and resolution times, escalation procedures, and any ongoing certificate management provisions. Comprehensive SLA with clear response times, escalation paths, and support coverage – 20 points Basic SLA with limited detail – 10 points Minimal or unclear SLA – 5 points No SLA provided – 0 points	20
4.	Project Implementation Plan Bidders must provide a high-level implementation plan outlining key activities, timelines, responsibilities, and approach to installation, testing, and go-live. Clear, detailed, and realistic implementation plan with timelines – 15 points Basic plan with limited detail – 10 points Vague or incomplete plan – 5 points No plan provided – 0 points	15

The minimum required points for the bidder to be considered for phase two is 70 points.

Any bidder scoring below the minimum threshold of 70 points will be regarded as non-responsive and therefore disqualified.