



TERMS OF REFERENCE

ONE (1) LOT SECURE SOCKETS LAYER (SSL) CERTIFICATE FOR THE GOVERNANCE COMMISSION FOR GOCCs (GCG)

1. SSL CERTIFICATE REQUIREMENTS

1.1 EXTENDED VALIDATION (EV) STANDARD

- 1.1.1 The bidder must provide three (3) EV SSL annual certificate and satisfies the minimum requirements and specifications below.
- 1.1.2 Certificate Specifications:
 - 1.1.2.1 Must have a Trust Level of Extended Validation (EV).
 - 1.1.2.2 Must have an organization name displayed in the web browser.
 - 1.1.2.3 Must have an Underwritten Warranty not be lower than One Million Five Hundred Thousand Dollars Only (\$1,500,000.00).
- 1.1.3 Feature Specifications:
 - 1.1.3.1 Must have a display of HTTPS (Secure Hyper Text Transfer Protocol) with padlock in web browsers.
 - 1.1.3.2 Must have a clickable Secure Site Seal.
 - 1.1.3.3 Must have a verified domain name.
 - 1.1.3.4 Must have an organization name displayed in the certificate.
 - 1.1.3.5 Must support Subject Alternative Name (SAN) options in the certificate.
 - 1.1.3.6 Must have a signature algorithm strength of SHA-256 with Elliptic Curve Cryptography (ECC) option.
 - 1.1.3.7 Must have a 2048-bit encryption strength in the certificate.
 - 1.1.3.8 Must support Transport Layer Security (TLS) version 1.2 in the cryptographic protocol.
 - 1.1.3.9 Must support both www.domain.com and domain.com (without the www).
 - 1.1.3.10 Must have unlimited SSL server licensing within certificate validity period.
 - 1.1.3.11 Must have unlimited reissuance to different servers/replacements.
 - 1.1.3.12 Must support all major web browsers for the root certificate.
 - 1.1.3.13 Must have browser to server and server to server authentication in the certificate.
 - 1.1.3.14 Must have 3-10 calendar days vetting turn-around for organization details.

1.2 ORGANIZATION VALIDATION (OV) WILDCARD REQUIREMENTS

1.2.1 The bidder must provide one (1) OV Wildcard SSL annual certificate and satisfies the minimum requirements and specifications below.

1.2.2 Certificate Specifications:

1.2.2.1 Must have a Trust Level of Organization Validation (OV).

1.2.2.2 Must have the secure top-level domain name as well as its 1st level sub-domains for the certificate.

1.2.2.3 Must have an Underwritten Warranty not be lower than One Million Two Hundred Fifty Thousand Dollars Only (\$1,250,000.00).

1.2.3 Feature Specifications:

1.2.3.1 Must have a display of HTTPS (Secure Hyper Text Transfer Protocol) with padlock in web browsers.

1.2.3.2 Must have a clickable Secure Site Seal.

1.2.3.3 Must have a verified domain name.

1.2.3.4 Must have an organization name displayed in the certificate.

1.2.3.5 Must support Subject Alternative Name (SAN) options in the certificate.

1.2.3.6 Must have a signature algorithm strength of SHA-256 with Elliptic Curve Cryptography (ECC) option.

1.2.3.7 Must have a 2048-bit encryption strength in the certificate.

1.2.3.8 Must support Transport Layer Security (TLS) version 1.2 in the cryptographic protocol.

1.2.3.9 Must support both www.domain.com and domain.com (without the www).

1.2.3.10 Must have unlimited SSL server licensing within certificate validity period.

1.2.3.11 Must have unlimited reissuance to different servers/replacements.

1.2.3.12 Must support all major web browsers for the root certificate.

1.2.3.13 Must have browser to server and server to server authentication in the certificate.

1.2.3.14 Must have 3-10 calendar days vetting turn-around for organization details.

2. BUDGET REQUIREMENTS

2.1 The budget for One (1) Lot Secure Sockets Layer (SSL) Certificate for Governance Commission for GOCCs (GCG) is Two Hundred Thousand Pesos Only (₱200,000.00).

3. BIDDER REQUIREMENTS

- 3.1 Must have a local technical support team.
- 3.2 Bidder must be a Platinum PhilGEPS registered supplier.
- 3.3 Subcontractors are prohibited.

4. SCOPE OF WORK AND SERVICE LEVEL AGREEMENT (SLA)

The Winning Bidder (hereafter referred to as simply the “bidder”) must:

- 4.1 perform the supply and delivery of annual (12 months) SSL certificates;
- 4.2 provide comprehensive user manual or guidelines, and assistance for setting-up the proposed SSL certificates;
- 4.3 provide a management portal for the purchased certificates with a feature to set unlimited number of user administrator;
- 4.4 provide a certificate inventory tool to local all SSL certificates for internal and public networks regardless of the issuing Certificate Authority (CA);
- 4.5 provide a notification tool for SSL certificate expirations; and
- 4.6 provide an SSL and website security checker with evaluation reports.
- 4.7 provide in-depth knowledge transfer on installation and management of SSL certificates to be conducted by a designated product expert.
- 4.8 provide full-time support and managed services as specified:
 - 4.8.1 eight hours by five days (8x5) service desk support via telephone, email or online chat portal;
 - 4.8.2 at least two (2) hour response time upon receipt of issue escalation and four (4) hours for onsite support, if applicable;
 - 4.8.3 procedures on support and issue escalation; and
 - 4.8.4 service report every after the onsite support.

5. TERMS OF PAYMENT

- 5.1 The payment shall be made on a one-time basis after the activation and deployment of the required SSL certificates.
- 5.2 Provided further that payment shall be made within twenty (20) working days upon receipt of complete documents such as billing statement/statement of account, and other pertinent documents.

6. CONFIDENTIALITY

- 6.1 Information or rights acquired and obtained from the GCG, including but not limited to any and all obligations prior to the termination or expiration hereof and provisions on confidentiality and proprietary rights, will remain in effect after termination of the services rendered to the GCG. Hence, the undertaking of the bidder not to disclose and to keep information confidential shall subsist even after the expiration or termination of its obligation to the GCG nor can the bidder, at any time, disclose items mentioned or enumerated in Section 6.2 or

any information it acquires by virtue of the contract which the GCG deems confidential.

- 6.2 Records, documents, reports, and relevant data such as diagrams, plans, designs, estimates, specifications, and other supporting records of materials compiled and prepared in the courses of the performance of the services shall be absolute properties of GCG and shall not be used by the bidder for purposes not related to this agreement without prior written approval of GCG. Copies of such documents as required in this TOR shall be turned over to GCG upon completion of the project except that the bidder shall have the right to retain a copy of the same.

7. DELIVERY AND IMPLEMENTATION SCHEDULE

- 7.1 The delivery and activation of proposed SSL certificates must be completed within thirty (30) calendar days from the receipt of the Notice to Proceed.
- 7.2 The bidder shall be subjected to the evaluation by the end-user after the implementation of the project.