Technical Evaluation Criteria – SSL Digital Certificate Services

Respondents must meet mandatory gatekeeper before their response can be evaluated. The minimum threshold required to pass the technical evaluation is 80%.

	#	Requirement	Evidence required	Response (Y/N)
Gatekeeper (Mandatory requirements)	1	The tenderer or/bidding company must have a proven track record for proving a cloud-based SSL certificate management service.	Provide a signed reference letter from the tenderer's customer confirming that the tenderer has provided a cloud-based SSL certificate management service and the duration.	

Category	#	Requirement	Weight	Response Y/N	Substantiate/ Indicate in RFP Response
Technical Evaluation Criteria	1	Does the solution create, issue, reissue, renew and revoke digital certificates from a central cloud-based console?	7% Has Central console= 7% No central console = 0		
	2	The solution must provide a self-service application designed to streamline external certificate management while providing secure certificates from an internationally recognised Certificate Authority.	11% Has Internationally recognised Certificate Authority = 11% No internationally recognised Certificate Authority = 0%		
	3	The proposed solution must have built-in workflow and approval controls to facilitate access requests and approvals.	7% Has built-in workflow = 7% No built-in workflow = 0%		
	4	The solution must have the ability to set certificate expiry dates to suit project schedules and corporate policies?	2% Can set certificate expiry = 2% Cannot set certificate expiry = 0%		
	5	Does the solution provide email notifications to ensure that certificates don't expire unexpectedly?	7% Has email notifications = 7% No email notifications = 0%		
	6	The solution must provide a comprehensive reporting capability for implemented digital certificates.	9% Has reporting capability = 9% No reporting capability = 0%		
	7	The solution must provide 24/7 local support for digital certificates with a dedicated account manager in South Africa.	10% 24/7 local support = 10% Limited local support = 5% No local support = 0%		
	8	The solution must be able to issue certificates that are trusted by Android and iOS mobile platforms.	5% Certificate trusted by iOS and Android = 5% Certificate not trusted by iOS and Android = 0%		

	9	The solution must provide a certificate discovery tool that can discover SSL certificates. In the local network as well as cloud.	9% Has certificate discovery tool for local and cloud = 9% No certificate discovery tool for local and cloud = 0%		
	10	SSL digital certificates provided must be trusted by prominent Web browsers in use such as Microsoft Edge, Mozilla Firefox, Google Chrome and the top mobile platforms.	2% Trusted by prominent Web browsers = 2% Not trusted by prominent Web browsers = 0%		
	11	The Certificate Authority (CA) must follow and practice the highest level of verification when applying for a SSL Certificate. Highest level acceptable is Organisational Validation (OV) and Extended Validation (EV) verification procedures.	4% Has OV and EV verification = 4% No OV and EV verification = 0%		
	13	The solution must offer a wide range of SSL certificates to meet every security need ranging from the basic OV SSL Certificate to multidomain certificates and Extended validation certificates.	4% Has range of SSL certificates = 4% No range of certificates = 0%		
	14	The solution must be able to support unlimited reissue of purchased certificates at no additional cost.	10% Support unlimited reissue of purchased certificates = 10% No support for unlimited reissue of purchased certificates = 0%		
	15	The solution must support modern encryption such as SHA2.	2% Supports modern encryption = 2% No support for modern encryption = 0%		
	16	The solution must provide a flexible subscription model which allows own selection of expiry dates and re-use certificate licenses to predict costs and provides flexibility.	11% Has flexible subscription model = 11% No flexible subscription model = 0%		
Total			**100%**		

Name: Ronald Netshishivhe

Requestor: Chief Advisor

Signature: _____

Date: 28/02/2023

Name: Charles Sello Kungwane

Supported by: Middle Manager Information Security

Signature: _____

Date: 28 February 2023