Sri Lanka CERT (Pvt.) Ltd

ADDENDUM NO 01 - TO THE BIDDING DOCUMENT

FOR THE

Procurement of CA system Solution for National Certification Authority

INVITATION FOR BIDS No: CERT/GOSL/GOODS/NCB/2024/21

September, 2024

ADDENDUM NO 01 - TO THE BIDDING DOCUMENT

INVITATION FOR BIDS No: CERT/GOSL/GOODS/NCB/2024/21

This Addendum to the Bidding Document of above procurement incorporates following amendments. All bidders shall comply with these amendments in addition to the clarifications issued.

Amendments

Sr.No.	RFP Reference	RFP Clause	Query	SL Cert Response
1	2. Evaluation Criteria (ITB 35.4) -> Commercial and Technical Capability -> iv.	Proposed solution has successfully implemented at least Three (03) similar software solution during the period of last Five (5) years prior to the Bid submission deadline (Bidder should be provided documents to prove the evidence). These products must be in satisfactory operation for at least One (1) year prior to the date of bid submission (Bidder should be provided documents to prove the evidence).	Please confirm if the Purchase Orders of the deployment should suffice as evidence for the deployment	Yes
2	Section IV. Bidding Forms -> Price Schedule	HSM - 3 Quantity OCSP - 3 Quantity	Please clarify if High availability feature is required for the CA infrastructure. According to the RFP section *"6.2. Resolution Time"* it is mentioned as mandatory. Considering this clause the number of HSMs mentioned might not suffice to provide the HA across Production and Backup sites for CA server. Adiditionally Purchaser to confirm - Signing keys of OCSP	Sri Lanka CERT requirement is to run the production site as active and DR site as pasive. According to the standard CA server should be kept in isolation and offline state. Any changes made to primary site CA server and its identical copy should be manually restored in DR CA server.

			Responder, in addition to CAs needs to be stored in HSM. - If HA is required in all sites.	
3	Section V. Schedule of Requirements -> 1. List of Goods and Delivery Schedule	The Bidder shall complete the Implementation, Configuration and Training within 12 weeks from the date of the contract	The deployment schedule is too short; of the 12 weeks, 8 to 10 weeks are needed for the supply of hardware and software. It would be challenging to finish all the other tasks in the remaining four weeks, including setting up the infrastructure, deploying the software, testing, going live, etc. We urge the Buyer to extend the deadline to twelve weeks following the receipt of H/W and HSM.	Should adhere to the RFP time line
4	Section V. Schedule of Requirements -> 1. 2. Technical Specifications	Pursuant to Gazette Extraordinary, 2147/58, dated 30th October 2019, Sri Lanka Computer Emergency Readiness Team (Sri Lanka CERT) has been designated as the Certification Authority under section 18 of the above Act to perform the functions of the NCA. Sri Lanka CERT intends to procure CA systems software and related services mentioned below.	1. Would you please clarify if the buyer plans to use the CA infrastructure to host the Root CA for Sri Lanka, which will be used exclusively for certifying Other Certification Authorities of SL, OR If this arrangement would be used to issue digital certificates to the SL public at large? 2. We strongly recommend the Purchaser to delete RA components from the list of technical specifications if the goal is not to provide DSCs to the general public.	Bidder should comply Sri Lanka CERT RFP requirement

5	2.1 TECHNICAL SPECIFICATIONS REQUIREMENT OF CA SYSTEM SOLUTION -> 2.1.1 Technical Specifications - CA SYSTEM -> CA software -> 29	Allows creation of Root CAs and Subordinate CAs	Assuming that the CA setup would involve issuing DSCs to the SL public, setting up an offline Root CA to supply certificates in real-time will be a laborious and time-consuming procedure. To facilitate the issusance process, we advise combining an online sub-CA configuration with an offline Root CA arrangement. Generally, a Sub-CA can be established and deployed as the Issuing CA while the Root CA certificate is kept in an offline arrangement. This setup will ensure online Sub-CA setup issues certificates based on the request received from from the RA setup, while maintaining the sanctity of the Rot CA setup. Note, necessary approvals can be setup in both RA & CA software. Kindly provide confirmation.	Bidder should comply Sri Lanka CERT RFP requirement
6	2.1 TECHNICAL SPECIFICATIONS REQUIREMENT OF CA SYSTEM SOLUTION -> 2.1.1 Technical Specifications - CA SYSTEM	RA Software		
7	4.General Compliance -> 4.1 General compliance -> 4.	The supplier is required to restore the latest copy of the primary CA system - offline zone onto the backup site offline zone server. This restoration must be completed following the implementation of any changes made to the CA system located in the primary site - offline zone.		
8	Annexture 02 Network and Zone Diagram	Offline Zone		
9	2.1 TECHNICAL SPECIFICATIONS REQUIREMENT OF CA SYSTEM SOLUTION -> 2.1.1 Technical Specifications - CA SYSTEM -> 7.	The proposed solution requirement shall be scalable as per the Sri Lanka CERT requirements and support allocating licenses to accommodate at the initial phase	Purchaser to confirm if there are any other requirements laid down by the SL CERT beyond those specified in the RFP	According to the proposed solution based on Sri Lanka CERT RFP bidder should have to submit.

10	2.1 TECHNICAL SPECIFICATIONS REQUIREMENT OF CA SYSTEM SOLUTION -> 2.1.1 Technical Specifications - CA SYSTEM -> CA software -> 30	Should support storing Digital keys in HSMs (Should compatible with proposed HSMs)	We presume this clause refers to storing of private keys of CAs in HSM. If any other private keys needs to be stored in HSM please mention.	Minimum 10 token keys per HSM should be provided by the bidder.
	2.1 TECHNICAL SPECIFICATIONS REQUIREMENT OF CA SYSTEM SOLUTION -> 2.1.1 Technical Specifications - CA SYSTEM -> CA software -> 38	e-Passport support for ICAO 9303, EAC 1.11, EAC 2.10 standards and latest	Please confirm if e-MRTD / EAC setup is also required. Should the bidder also bid for the corresponding components required for setting up e-Passport issuance like CSCA, CVCA, DS, DV, etc. If yes, then we urge the purchaser to consider having two seperate physical setup. Please confirm	Bidder should comply Sri Lanka CERT RFP requirement.
11	2.1 TECHNICAL SPECIFICATIONS REQUIREMENT OF CA SYSTEM SOLUTION -> 2.1.1 Technical Specifications - CA SYSTEM -> CA software -> 39	Should support TSA (specify the supported products)	As TimeStamping Authority software is not listed as part of the tender, we presume the purchaser has an exisiting TSA service running. We presume the software is designed based on RFC & industry standards. Please confirm the above points or if TSA has to be delivered	Sri Lanka CERT doesn't have any TSA software. Bidder should proposed new TSA software and associated components
12	2.1 TECHNICAL SPECIFICATIONS REQUIREMENT OF CA SYSTEM SOLUTION -> 2.1.1 Technical Specifications	The equipment/software quoted by bidder should not be declared as End of Life (EOL) or End of Sale (EOS) by the OEM, for a period of 5 years from the last date of RFP.	Please confirm if the EOL & EOS is required for 5 years / 8 years. As OEM offering EOS / EOL for 8 years is not practically	5 Years for Servers & 8 Years for HSM

	- CA SYSTEM -> CA software -> 24		possible due to the evolving nature in Information security space. Hence we urge the purchaser to match it with the AMC period, subsjected maximum to 5 years	
13	4. General Compliance -> 4.1 General compliance -> 15.	Certification from the manufacturer or main authorized distributor in the Sri Lanka that all proposed items will not reach its END-OF-LIFE (products) and END-OF-SUPPORT (services) in 8 years' time from the date of award of contract.		
14	Generic	Migration	Please confirm if there is an exisiting setup and any migration is required as part of the Scope of Work. If yes, then detailed note on the exisitng setup and migration activity needs to be furnished by the Purchaser.	migration is not required
16	Generic	Volumetrics	Purchaser to provide the following details to provide an optimum hardware siziing for the CA setup : No of Certificates exptected to be issued (Per year / for 3 years) : HA required : Y / N, if yes do all sites require it CA TPS expected : OCSP requests-Response expected : OCSP TPS expected :	Bidder should comply Sri Lanka CERT RFP requirement.

17	4. General Compliance -> 4.1 General compliance -> 13	Bidder shall allocate qualified dedicated personnel or team 24x7 to directly communicate with Purchaser technical team to resolve all technical issues and carry out technical improvements within the contract period. Bidder should provide single point of contact & proper escalation matrix	The requirement for round-the-clock support seems excessive given that the infrastructure is being set up for the National Certifying Authority, which certifies other CAs. We propose amending the clause to provide assistance during business hours from 9 to 5 p.m.	Bidder should comply Sri Lanka CERT RFP requirement.
18	6.2. Resolution Time	**Critical Incidents** Resolution Time - 2 hours “Resolution time” is amount of time between when the Purchaser first report an incident and when that problem is actually solved Penalty - If Monthly availability is less than 99.98 % (Total downtime 8 minutes), 0.2% of Total contract value will be charged for additional one hour of downtime on an incremental basis	We urge Purchaser that the resolution time be changed to 24 hours for critical incidents and 48 hours for high incidents, as we have a disaster recovery setup and the main goal of the solution is to certify authorities where activity will occur infrequently, as opposed to issuing certifications to the general public.	Bidder should comply Sri Lanka CERT RFP requirement.
19		**High Incident** *Resolution Time* - 6 hrs. “Resolution time” is amount of time between when the Purchaser first report an incident and when that problem is actually solved *Penalty* - 0.02 % of the Total Contract value for every one hour of delay after initial six (6) hours on an incremental basis per high incident.		

20	Generic	Technical Compliance	Given that the solution is utilized for the certification of other CAs, we suggest the buyer modify the technical, functional, and overall compliance in line with the NCA scope of work. The current compliance is oriented primarily toward establishing a CA infrastructure for public certificate issuance.	Bidder should comply Sri Lanka CERT RFP requirement.
21	HSM	Pricing Schedule	In the table below, it is mentioned only 3 HSMs but they also have 3 environments(Prod, Backup, Staging), kindly help in with the distribution of the HSMs?	Production - 01 DR - 01 Staging - 01
22		TSA	TSA is mentioned as required in the tender doc but couldn’t see it in the architecture. Please provide additional information for this.	Sri Lanka CERT doesn't have any TSA software. Bidder should proposed new TSA software and associated components