केनरा बैंक Canara Bank

Corrigendum-1 to GeM Bid ref no. GEM/2024/B/5004512 dated 01/06/2024 for Selection of Service Provider for Supply, Installation, Migration and Maintenance of Payment Hardware Security Module (HSM) in Canara Bank for 5 Years.

It is decided to amend the following in respect of the above GeM bid:

a. GeM bid document (Bid End date/ Bid Opening Date, Page no. 1 of 7):

Description	Existing details	Amended details
Bid End Date/Time	24/06/2024, 15:00:00	26/06/2024, 15:00:00
Bid opening Date/Time	24/06/2024, 15:30:00	26/06/2024, 15:30:00

b.

Sl No.	Section/Annexure/Appendix of GeM Bid	Clause No.	Existing Clause	Amended Clause
1	Annexure 10: Technical Requirement	Annexure 10: Technical Requirement	Existing Annexure	Amended Annexure10: Technical Requirement attached along with this Corrigendum.

All the other instructions and terms & conditions of the above GeM Bid shall remain unchanged.

Please take note of the above amendments while submitting your response to the subject GeM bid.

Date: 18/06/2024

Place: Bengaluru

Deputy General Manager

केनरा बैंक CANARA BANK Centralized Procurement & Vendor Management Wing H.O., Bengaluru-560001 केंद्रीकृत खरीद एवं विक्रेता प्रबंधन विभाग, प्र.का., बेंगलूरु-560001

Annexure-10

Technical Requirement

SUB: RFP for Selection of service provider for Supply, Installation, Migration and Maintenance of Payment Hardware Security Module (HSM) in Canara Bank

Ref: GEM/2024/B/5004512 dated 01/06/2024.

Bidder's capability including proven relevant experience and capabilities of identified professionals for the project" is given below:

Note:

1. The bidder shall specifically mention the make and model of the items offered for all the requirements in terms of GeM Bid without fail, failing which the bid is liable for rejection.
2. If the bidder feels that certain features offered are superior to what has been specified by the Bank, it shall be highlighted separately. Information regarding any modification required in the proposed configuration to meet the intent of the specifications and state-of-the-art technology shall be provided. However, the Bank reserves the right to accept the modifications / superior features suggested/offered.
3. The bidder shall provide all other required equipment and services, whether or not explicitly mentioned in this GeM Bid, to ensure the intent of specification, completeness, operability, maintainability and upgradability.
4. The selected bidder shall own the responsibility to demonstrate that the products offered are as per the specification/performance stipulated in this GeM Bid and as committed by the bidder either at site or in bidder's work site without any extra cost to the Bank.

Technical Specification of Payment Hardware Security Module (HSM)

All points mentioned in scope of work are mandatory to comply and non-compliance to any of the point lead to disqualification of the bidder during evaluation.

Sl. No.	Technical Specification for Payment HSM	Compliance (Yes/No/ Specify)	Remarks/ Details
1	Make:		
2	Model:		
3	Speed:25 to 100 TPS/CPS (Transactions per second/Calls persecond)		
General Aspects			
4	The proposed payment HSM should have dual hot-swappable power supply and fans, dual TCP/IP interface and dual connectivity support.2 IEC Male to Female power cords.		
5	The proposed payment HSM must be PCI-HSM 3.0 Certified or above		
6	The proposed payment HSM must be FIPS140-2 Level 3 Certified or above with ACTIVE status.		

Centralized Procurement & Vendor Management Wing

Sl. No.	Technical Specification for Payment HSM	Compliance (Yes/No/ Specify)	Remarks/ Details
7	The proposed payment HSM should support SHA-256 RSA 2048 Format or above. Capable to support DES and 3DES KEY lengths 112bit &168 bit and AES key lengths 128, 192 & 256 bits.		
8	**Capable of translating up to at least 25 PIN triple DES/AES Pin block Per Second.**		
9	**The proposed payment HSM should support multi-threading so as maximum performance can be achieved.**		
10	The proposed payment HSM should support following Crypto Graphic Standard: AES, DES and Triple DES Algorithms - Provide PIN encryption, PIN Authorization and message authentication capabilities.		
11	The relevant security settings in the firmware should have PCI compliant values		
12	Shipment of the payment HSM should be compliant as per PCI HSM requirement		
Management facilities:			
13	**Should have GUI/CLI available with 2 factor Authentication using USB Tokens or Smart Cards.**		
14	Support SNMP		
15	Utilization statistics - Health check diagnostic and error logs		
16	Payment HSM should have dedicated management Ethernet port and must have Secure Host Communications Management Option for TLS authenticated sessions on Ethernet hostport.		
Key Managements:			
17	Key Block support (superset of ANSI X9.24) or Higher		
18	DUKPT (DES and Triple-DES) Support		
Security Certification:			
19	**Cryptographic module certified to FIPS: 140-2 Level 3, 186-4, 198 or higher.**		
20	PCI HSM 3.0 Standard or above		
21	SP800-90(A)		
22	FIPS approved Random number generator		
23	FIPS approved algorithms		
Security features:			
24	Tamper resistance meeting requirements of PCI HSM 3.0 &FIPS 140-2 Level 3 or higher		
25	**Alarm triggers for Voltage and alert trigger for temperature and other alerts as per FIPS 140-2 Level 3 or higher compliance.**		

केनरा बैंक CANARA BANK Centralized Procurement & Vendor Management Wing H.O. Bengaluru-560001

Sl. No.	Technical Specification for Payment HSM	Compliance (Yes/No/ Specify)	Remarks/ Details
26	Alarm triggers for Voltage and alert trigger for temperature and other alerts as per FIPS 140-2 Level 3 or higher compliance.		
27	Device hardening - ability to disable functions not required by the host application		
28	Audit trails and 2 Factor Authentication for Auditor using USB tokens / Smart Cards.		
29	DES and Triple-DES key lengths 112 & 168 bit		
30	AES key lengths 128, 192 & 256 bit		
31	RSA (up to 4096 bit)		
32	HMAC, MD5, SHA-1, SHA-2		
Key Features:			
33	Reporting of Authorization State identifies whether commands are Host, Console, or All		
34	Secure Key Storage and Generation for all key types used		
35	Reduced Key check value: 6 HEX		
36	Encrypted decimalization table		
37	Secure Host communication using TLS or SSL		
38	PIN never appears in the clear outside of a tamperresistant security module as per PCI PIN security requirements		
39	Key Entry Mechanism are protected as per PCI HSM 3.0 requirements		
40	Remote management and monitoring options.		
41	Multiple LMK options - at least 20 partitions per HSM		
42	Safety and environmental compliances UL, UL/CA, UL-AR,CE, BIS, FCC, Canada ICES, RCM, KC, VCCI RoHS2, REACH, WEEE		
Financial services standards			
43	ISO: 9564, 10118, 11568, 13491, 16609		
44	ANSI: X3.92, X9.8, X9.9, X9.17, X9.19, X9.24, X9.31, X9.52, X9.97		
45	ASC X9 TR-31, X9 TG-3/TR-39		
46	APACS 40 & 70		
Other Features			
47	Should provide authenticated multi-role access control		
48	Must have strong separation of administration and operator roles		
49	Must have secure key wrapping, backup, replication and recovery.		
50	Must support 2048, 4096 bits RSA private keys, 256 bits AES keys on FIPS 140-2 Level 3 or higher Certified Memory of Cryptographic Module		
51	Must support clustering and load balancing		

Sl. No.	Technical Specification for Payment HSM	Compliance (Yes/No/ Specify)	Remarks/ Details
52	Should support cryptographic separation of application keys using logical partitions		
53	Must support M of N multi-factor authentication		
54	Minimum Dual port (1 Gbps) supporting TCP/IP & UDP protocols.		
55	Asymmetric public key algorithms: RSA, Diffie Hellman, DSA, ECDSA, ECDH		
56	Symmetric algorithms: AES, Triple DES, HMAC		
57	Hash/message digest: SHA-1, SHA-2 (224,256,384,512 bit)		
58	Support remote administration - including adding applications, updating firmware, and checking status fromcentralized Location		
59	Syslog/Snmp diagnostics support		
60	Command line interface (CLI/graphical user interface (GUI))		
61	Support SNMP monitoring agent.		
62	Should be upgradable to at least 1000 TPS/CPS		
63	Should be compatible to existing payment HSM for smooth migration of keys (including LMK) and custom firmwares without the risk of keys coming out in clear out of HSM		
64	There should not be any changes required in the application/hardware device currently integrated with existing payment HSMs like ATM Switch/Mobile Banking/UPI or Credit Card Switch.		
65	HSM remote management solution must have PCI HSM v3 Remote Access Platform (RAP) certification		
66	Payment HSM should have Dual Physical lock along with console cables		
67	Form Factor - 1U/2U rack mount - standard wide rack mountable with rail kit adjustable depth.		
68	Voltage - 90 to 264 VAC		
69	Power Consumption- 40W or higher but not more than 100W		
70	Temperature Range 10 deg C to 70 deg C		
71	Should have ability to regularly expand functionality via firmware or application upgrades.		
72	Should have physical and logical security features.		
73	Should adhere to the major industry standards, including FIPS-140-2 level 3, PCI-DSS.		

Sl. No.	Technical Specification for Payment HSM	Compliance (Yes/No/ Specify)	Remarks/ Details
74	Should have multiple, redundant power supplies and Ethernet ports to maintain functionality in the event thatone of the either sources should fail.		
75	The solution must have added ability of being spread across multiple locations and managed as a group, synchronizing and load balancing all the units to maintainnetwork functionality even if an entire data center were to lose connectivity		
76	Payment HSM should support remote access technology with encrypted connection to maintain security in all configuration and remote key loading processes.		
77	Payment HSM must maintain compatibility with wide range of host applications		
Common Uses - Should support following common uses			
78	Payment credential issuing - cards, mobile secure elements, wearable's, connected devices and host card emulation (HCE) applications		
79	PIN Routing		
80	Point to Point Encryption (P2PE)		
81	Security Tokenization (for PCI DSS compliance)		
82	EMV Payment tokenization		
83	Card and Mobile payment authorization		
84	POS, mPOS and SPoC key management		
85	PIN and EMV cryptogram validation		
86	Remote Key Loading & Management		
Card/Mobile payment support - should support the needs of leading payment brands (RuPay, JCB, VISA, MasterCard, UnionPay, American Express) in number of areas including			
87	PIN and card verification functions for all major payment brands		
88	EMV transaction authorization and messaging		
89	Mobile payment transaction authorization and messaging		
90	Remote key loading for ATM and POS devices		
91	Local/Global key Management		
92	Master Card On-Behalf key management (OBKM) Support		
93	PIN generation and printing		
Remote Management			
94	Should have option to Operate from Remote Console and GUI		
95	Perform operational activities in secure manner like Authorization, Key Generation, Changing HSM		

Sl. No.	Technical Specification for Payment HSM	Compliance (Yes/No/ Specify)	Remarks/ Details
	parameters		
Logical Security			
96	Local Master Key (LMK) options - variant and key block		
97	Two factor authentication (2FA) of security officers using smart cards		
98	Strongest security settings implemented by default		
99	Audit logs with user control over the scope of events recorded		
100	LMK Component Cards (6 Blank Cards per HSM)		

Terms & Conditions

a. Bank reserves the right to conduct interviews of the proposed team members.

b. In case of absence of the allotted resource, the standby should perform the job of the absentee.

c. Bank may reject such manpower if bank is not satisfied with his/her performance.

Declaration: We hereby confirm that the information submitted above is true to the best of our knowledge. We understand that in case any discrepancy is found in the information submitted by us, our response to this RFP is liable for rejection.

Date:

Signature with seal
Name:
Designation :

केनरा बैंक CANARA BANK Centralized Procurement & Vendor Management Wing H.O. Bengaluru-560001 केन्द्रीकृत क्रयण एवं विक्रेता प्रबंधन विभाग, प्र.का., बेंगलूरु-560001