केनरा बैंक Canara Bank

Corrigendum-1 to GeM bid ref no. GEM/2024/B/5016455 dated 05/06/2024 for Selection of Vendor for Implementation of Comprehensive Card-On-File Tokenization Solution for Generation of CoF Tokens for a Card in Canara Bank On OPEX Model for a Period of 3 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	27-06-2024, 15:00:00	29-06-2024, 15:00:00
Bid Opening Date/Time	27-06-2024, 15:30:00	29-06-2024, 15:30:00

Sl. No.	Page No.	Section/ Annexure/ Appendix of the RFP	Clause No.	Existing	Amended
b.	57	Annexure-2	Pre-Qualification Criteria	Pre-Qualification Criteria	Amended Pre-Qualification Criteria.
c.	68	Annexure-9	Scope of Work	Scope of Work	Modified Scope of Work
d.	78	Annexure-13	Bill of Material	Bill of Material	Amended Bill of Material.
e.	81	Annexure-14	Undertaking of Authenticity	Undertaking of Authenticity	Amended Undertaking of Authenticity.
f.	82	Annexure-15	Manufacturer Authorization Form	Manufacturer Authorization Form	Amended Manufacturer Authorization Form.
g.	83	Annexure-16	Letter for EMD Return	Letter for EMD Return	Amended Letter for EMD Return

केनरा बैंक CANARA BANK Tender Processing Section C.P.&V.M. Wing, H.O.

h.	20	Section-C	Scope involved during Contract period.	9.5 The support shall be given in **person**/email/fax/tele/remote access.	9.5 The support shall be given through email/fax/tele/remote access.

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: 21/06/2024
Place: Bengaluru

Deputy General Manager

केनरा बैंक CANARA BANK Tender Processing Section C.P.&V.M. Wing, H.O., Bengaluru सी. पी. एवं वी. एम. विभाग, प्र.का., बेंगलूरु - 560 001

केनरा बैंक Canara Bank

Annexure-2
Pre-Qualification Criteria

[On Firm's / Company's letter head]

SUB: RFP for Selection of Vendor for Implementation of Comprehensive Card-On-File Tokenization Solution for Generation of CoF Tokens for a Card in Canara Bank On OPEX Model for a Period of 3 Years

Ref: GEM/2024/B/5016455 dated 05/06/2024.

We have carefully gone through the contents of the above referred GeM bid replies to pre-bid queries and amendments, and furnish the following information relating to Technical Criteria.

Sl. No.	Criteria	Documents to be submitted for Compliance	Bidder's response and documents Submitted
1.	Signing of Pre-Contract Integrity Pact	The bidder should submit signed Pre-Contract integrity pact on Non-Judicial Stamp Paper of Rs.500/- or more (as per respective state Stamp Act) as per Appendix-F.	
2.	The bidder (including its OEM, if any) should either be Class-I or Class-II local supplier as defined in Public Procurement (Preference to Make in India) Revised Order (English) dated 16-09-2020.	Certificate of local content to be submitted as per Annexure-5.	
3.	The bidder should provide confirmation that any person/ Partnership/ LLP/ Company including any subsidiary or holding company/ proprietorship connected to bidder directly or indirectly has not participated in the bid process.	The bidder should submit letter of confirmation on the Company's letter head to this effect.	
4.	The Bidder should be either a partnership firm registered under LLP Act, 2008/Indian Partnership Act, 1932 or Company in India as per Indian Companies Act, 1956 or Indian Companies Act, 2013 and should have been in operation for at least five years as on GeM bid date.	Copy of Certificate of LLP registration. (OR) Copy of Certificate of Incorporation and Certificate of Commencement of business in case of Public Limited Company (OR) Certificate of Incorporation in case of Private Limited Company, issued by the Registrar of Companies.	

Sl. No.	Criteria	Documents to be submitted for Compliance	Bidder's response and documents Submitted
5.	The bidder should have a minimum annual turnover of Rs.1.5 Crores during last 3 financial years (i.e. 2019-20, 2020-21 & 2021-22) from Indian operations. This must be the individual company turnover and not of any group of companies.	Bidder should submit Audited Balance Sheet copies for last 3 financial years i.e. 2019-20, 2020-21 and 2021-22 along with certificate from the Company's Chartered Accountant to this effect with Unique Document Identification Number.	
6.	The bidder should have positive Net Worth as on 31/03/2023 and also should have not eroded by more than 30% in the last three financial years.	The bidder must produce a certificate from the Company's Chartered Accountant with UDIN to this effect.	
7.	Bidder should be the Original Equipment Manufacturer (OEM)/ Original Software Owner (OSO)/ Original Software Developer (OSD) of Solution. (OR) An authorized dealer/distributor of the proposed Solution	If the applicant is OSD/OSO, an Undertaking Letter has to submit in this effect. (OR) If the bidder is an authorized dealer/ distributor, an authorization letter from their OEM and OSO/ OSD to deal/market their product in India and it should be valid for entire contract period from the date of submission of the bid.	
8.	**The bidder/OEM should have implemented/implementing and maintaining Card-On-File Tokenization Solution in schedule commercial Public/ Private Banks with minimum 500 branches in India as on RFP date.**	The bidder should submit purchase Order and reference letter for the solution duly mentioning the number of branches being used.	
9.	**The proposed Card-On-File Tokenization Solution should have been implemented and being used or implementing in schedule commercial Public/ Private Banks in India having customer base of minimum Ten Lakhs (10,00,000).**	The bidder should submit purchase order and reference letter duly mentioning that the supplied Card-On-File Tokenization Solution is being used and working satisfactorily to this effect.	
10.	The bidder should have certified with all the three card networks (Visa/Master/ NPCI) for Card-On-File Tokenization	The bidder should submit documentary evidence to this effect from respective Card networks.	

Sl. No.	Criteria	Documents to be submitted for Compliance	Bidder's response and documents Submitted
11.	Bidders should not be under debarment/blacklist period for breach of contract/fraud/corrupt practices by any Scheduled Commercial Bank/ Public Sector Undertaking / State or Central Government or their agencies/ departments on the date of submission of bid for this GeM bid.	A self-declaration letter by the bidder on the Company's letter head should be submitted.	
12.	Any Bidder (including OEM and OSD/OSO, if any) from a country which shares a land border with India will be eligible to bid, only if the Bidder (including OEM and OSD/OSO) are registered with the Competent Authority. Bidder (entity) from a country which shares a land border with India means: a. An entity incorporated, established or registered in such a country; or b. A subsidiary of an entity incorporated, established or registered in such a country; or c. An entity substantially controlled through entities incorporated, established or registered in such a country; or d. An entity whose beneficial owner is situated in such a country; or e. An Indian (or other) agent of such an entity; or f. A natural person who is a citizen of such a country; or g. A consortium or joint venture where any member of the consortium or joint venture falls under any of the above.	A declaration stating "We have read the clause regarding restrictions on procurement from a Bidder of a country which shares a land border with India. We further certify that we and our OEM are not from such a country or if from such a country, has been registered with Competent Authority. We hereby certify that we and our OEM fulfills all requirements in this regard and are eligible to be considered" to be submitted in Company's letter head. [Where applicable, evidence of valid registration by the Competent Authority shall be attached.]	
13.	Authorization Certificate - Whether the Bid is authenticated by authorized person.	Bidder to submit a copy of the Power of Attorney or the Board Resolution and KYC documents evidencing the authority delegated to the authorized signatory.	

Sl. No.	Criteria	Documents to be submitted for Compliance	Bidder's response and documents Submitted
14.	The bidder should have a valid PA/PCI DSS certification as on RFP date for the propose solution.	The bidder should submit a copy of the Certificate to this effect.	
15.	The bidder should have support office in Bengaluru or Mumbai for 24x7 supports.	The Bidder should submit the details viz., address, phone no., email id and contact person Name & Mobile no. etc., as per Annexure-8.	

We confirm that the information furnished above is true and correct. We also note that, if there are any inconsistencies in the information furnished above, the bid is liable for rejection.

Date:

Signature with seal
Name :
Designation :

Annexure-9

Scope of Work

(Should be submitted on Company's letter head with company seal and signature of the authorized person) (To be included in Part A- Eligibility cum Technical Proposal)

SUB: RFP for Selection of Vendor for Implementation of Comprehensive Card-On-File Tokenization Solution for Generation of CoF Tokens for a Card in Canara Bank On OPEX Model for a Period of 3 Years.

Ref: GEM/2024/B/5016455 dated 05/06/2024.

The scope of work shall broadly cover Installation Configuration & Integration of the Card-On File Tokenization through issuer banks and the said solution should be integrated with banks Internet Banking and Mobile Banking systems at both PRIMARY & DR sites of CANARA BANK.

1. Generation of Cof Tokens for a card, through the card issuer, can be enabled through mobile banking and internet banking channels.
2. CoFT generation shall be done only on explicit customer consent, and with AFA validation. If the cardholder selects multiple merchants for which to tokenise his/her card, AFA validation may be combined for all these merchants.
3. The tokens thus generated shall be made available on the merchant's payment page, in the cardholder's account with the merchant.
4. The cardholder may tokenise the card at any time of his convenience, either on receipt of the new card or later.
5. The card issuer shall provide a complete list of merchants for whom it can provide tokenisation services. The cardholders shall select the merchants with whom he/she wishes to maintain tokens. (Alternatively - "The gardholder can make his selection from the list").
6. The card token so issued may be either by the card network or the issuer or both.

CoFT through card issuers - Requirements

1. Generation of CoF Tokens for a card, through the card issuer, can be enabled through mobile banking and internet banking channels.
2. CoFT generation shall be done only on explicit customer consent, and with AFA validation. If the cardholder selects multiple merchants for which to tokenise his/her card, AFA validation may be combined for all these merchants.
3. The tokens thus generated shall be made available on the merchant's payment page, in the cardholder's account with the merchant.
4. The cardholder may tokenise the card at any time of his convenience, either on receipt of the new card or later.
5. The card issuer shall provide a complete list of merchants for whom it can provide tokenization services. The cardholders shall select the merchants with whom he/she wishes to maintai tokens. (Alternatively - "The cardholder can make his selection from the list").*
6. The card token so issued may be either by the card network or the issuer or both.

7. All other provisions of RBI circulars dated January 8, 2019, August 25, 2021, September 7, 2021 and July 28, 2022 shall remain applicable.

Cloud Security Checklist to be submitted by bidder

Sl No	Check List	Compliance (Yes/No)
1.	The CSP for the deployments should be a MeitY (Ministry of Electronics and Information Technology) empanelled Cloud Service Provider	
2.	Research and assess the potential of the CSP/TSP vendors for their security capabilities and reputation	
3.	Bidder to ensure that the CSP is chosen such that CIS Benchmark prescribed configuration recommendations are available in CIS (Center for Internet Security).	
4.	Bidder to ensure that the CSP is chosen such that they are compliant with the requirements as stated in the latest standard of CSA STAR CCM *(Currently v4.0 as on date of release of this document).* The listing of the CSP compliance to CSA STAR CCM can be checked at https://cloudsecurityalliance.org/star/registry/	
5.	The TSP/CSP to ensure that baseline security configuration of Operating System, Database, Web Server etc. is in accordance with the industry best practices preferably CIS Based benchmark images.	
6.	CSP/TSP should comply to the detailed cloud security best practices published on website of MeitY at following URL: https://www.meity.gov.in/writereaddata/files/2.%20WI3_Cloud%20Security%20Best%20Practices_06112020.pdf	
7.	The data should be stored within geography of India.	
8.	The CSP/TSP to ensure that they would comply to the Reserve Bank of India issued a directive vide circular DPSS.CO.OD.No 2785/06.08.005/2017-18 dated April 06, 2018 on 'Storage of Payment System Data' advising all system providers to ensure that the entire data relating to payment systems operated by them is stored in a system only in India.	
9.	CSP/TSP should ensure establishing necessary DC and DR Setup in multiple seismic zone separated geo-graphical areas.	
10.	In single region also, multiple availability zones should be available and setup for redundancy and fault tolerance purposes.	
11.	All functions involving critical and PII data to be maintained on-premises only while functions involving non critical data can be moved to Cloud thereby adopting Hybrid Cloud model approach.	

12.	**Key Management:** The CSP/TSP should provision and utilize management service that stores and manages master encryption keys and secrets for secure access to resources. a. Encryption keys which are used for encryption in cloud should support BYOK (Bring Your Own Keys) and use along with KMS (Key management Service). b. The encryption keys to be exchanged over a secure channel and the keys must be properly secured using KMS and be accessible to the appropriate application/services on a need to know basis using properly defined IAM Policies. c. The CSP should support regular rotation of encryption keys and certificates and TSP has to configure accordingly.	
13.	**IAM (Identity Access Management) Controls:** a. IAM controls, roles, IAM groups, policies to be configured for all the resources, users etc. based on principle of least privilege and are regularly reviewed. b. For administration purposes, privileged accounts, user login and for any critical actions ensure MFA is in place as an additional layer of security of the IAM users and roles. c. Zero Trust security model approach to be ensured.	
14.	**Security/Landing Zone:** The CSP should have provision for creation and configuring security zones such that resources like compute, networking, object storage, block volume and database resources etc.	
15.	**Security Patches and Updates:** CSP/TSP should ensure updating their systems/ resources/ application/ instances/ hardware with the latest security patches to maintain a secure Cloud infrastructure.	
16.	CSP should provide secure repository of the digital certificates etc.	
17.	**Data Encryption:** Ensure data in rest and transit are encrypted with strongest industry standard encryption algorithms.	
18.	The CSP should be able to provide geographic or IP based restrictions.	
19.	**Incident response and disaster recovery:** Ensure the CSP/TSP has well-defined incident response plan in place to quickly and effectively respond to security incidents and minimize their impact, and regularly test your disaster recovery procedures.	
20.	**Data Backup:** CSP/TSP should ensure robust, consistent and regular back-up and recovery/data restoration plans are in place. The data & configuration backups are to be taken in fully encrypted mode and maintained as per the Bank's policy/procedure.	
21.	**Logging and auditing:** The CSP/TSP should enable detailed logging and auditing of user, process activities & other activities in all resources including when and how data is accessed, changes in policy assignments, privileged accounts, administration actions and authorization logs which may indicate sensitive or privileged actions, to help detect and respond to security incidents.	

22.	**Continuous Monitoring:** a. CSP/TSP to ensure continuous monitoring of audit, events, access to critical data and/or processes, or other change/activity logs. b. Bank Teams also to be given login for dashboard	
23.	**Security Incident Event Monitoring (SIEM):** a. The alerts, logs, events from CSPs should be able to integrate with Bank's incident response process i.e SOC wherever applicable and/or retention of relevant logs in cloud shall be ensured for incident reporting and handling of incidents relating to services deployed on the cloud. b. The CSP/TSP should establish a dedicated or managed SOC Team for ensuring security incident monitoring on 24x7 basis and effectively respond and remediate to security incidents.	
24.	**Cloud Security Posture Management (CSPM):** The CSP should support cloud native service that helps bank to monitor, identify, achieve and maintain a strong security posture on the cloud. It should also allow examining cloud resources for security weakness related to configuration, operators and users for risky activities. Also upon detection, the native service can suggest, assist or take corrective actions.	
25.	**Data Portability:** Ensure that CSP/TSP is flexible by providing suitable options such that data can be easily and seamlessly migrated in case if bank decide to switch to another CSP/TSP.	
26.	The CSP/TSP shall ensure for the below i. The security for hypervisors, containers and Software defined networks ii. Proper and adequate incident detection, response, notification and remediation. iii. Strong perimeter security for API gateways and web consoles iv. MFA v. Assure security isolation between tenants **vi. Configure hypervisors to isolate VMs/Containers from each other** vii. Implement processes and technical security controls to prevent admin/non-tenant access to running VMs or volatile memory. viii. Encrypt underlying physical storage **ix.** Role based access controls and strong authentication for all container and repository management	

Bidder to agree the following security related points to be included in the SLA and agreement with the Bank.

Sl No.	Agreement	Compliance
1.	As per the cyber security guidelines by RBI, Bank, and the Regulatory authorities should have access to their IT infrastructure as and when required for audit from security perspective which may also include visits without prior notice to ensure Bank's data are not misused	
2.	Third parties/partners/TSP/CSP are also conducting background check, ensuring regular security assessments, audits on their suppliers, vendors and other third-party partners as well as employees (third-party risk management program)	

3.	Clauses for not only the uptime, but also for the confidentiality and integrity of the underlying data.	
4.	Right to Audit clause in place, in agreement with the vendor/TSP/CSP for performing audit or other assessments & security assessment for the associated infrastructure	
5.	Right to monitor and right to terminate services in the event of a security incident or a security breach	
6.	Clauses to protect Bank's interest and to enforce optimum controls as per the Bank's policy. Vendor/Service provider/TSP/CSP should be bound to a Non-Disclosure agreement and maintain incident reporting to Bank in case of any eventuality	
7.	Clauses Data Retention, Masking of Data, Archiving, Destruction of data, Sharing of Data, Encryption of critical data etc.	
8.	The CSP shall adhere to all laws pertaining to data privacy and protection that are applicable as per GoI, RBI and any other regulators	
9.	The CSP shall also ensure that necessary enhancements are made to the services provided whenever there are changes sought either by the regulators or Government of India	
10.	In case of any breach vendor/Service provider should notify bank and regulators immediately and provide RCA and take appropriate action, remediate and cooperate for Incident Management	
11.	**Business Continuity:** The SLA should clearly reflect RTO (Recovery Time Objective) and RPO (Recovery Point Objective), MTD (Maximum Tolerable Downtime), uptime and performance parameters and alternatives for contingency situations for provider infrastructure (including network)	
12.	CSP/TSP vendor has to provide all the Audit Certifications on data center, data security and access control of the cloud deployment	
13.	Ensure proper SLAs in place and certificates are also obtained covering third party vendor/Service/TSP/CSP provider that their systems are at minimum complied to security best practices such as a. Regular conducting VAPT, API Assessment, Source Code audit certified by a CERT-IN empaneled auditor. b. Regular Hardening of System preferably CIS Benchmark, System & Application Patching to latest release patches and security updates c. Adhering to NIST (especially 800-53) and CSF (Cyber Security Framework) standard best practices. d. Monitoring CERT-IN and any other regulator's released advisories and fixing applicable vulnerabilities. e. Certified for PCI DSS (For Applications wherever Card Data and Transactions are involved) f. SOC-II	

	g. Security Training and Awareness: The employees as well as vendor staff received security and security awareness training. **h.** Conduct third party risk assessment on regular basis and monitor for any data breach /leak cases from supply chains to take necessary protective & remedial measures	
14.	**Termination rights and process / Exit strategy:** a. Agreement to consider data deletion including backups and residual data/metadata (ex: system logs, audit logs, access logs, search indices), timelines and written notification of successful deletion. b. Agreement should define exit strategy in the event of termination of the outsourcing agreement	
15.	The agreement shall provide for ensuring prior approval/consent by the bank for engaging any outsourcing or sub-contractors by the service provider for all or part of the activity	
16.	The CSP to ensure that the CSP complies with all the necessary security and Data Protection regulations such as Digital Personal Data Protection Act (DPDP), 2023 and the RBI's guidelines on Data Storage and handling	
17.	the vendor TSP/CSP/vendors undertakes to remedy any observations reported by RBI/external vendors on cloud operations	
18.	to provide support/coordinate/undertake necessary activities for smooth transfer of data/applications/APIs in event of reverse migration to on-premises of the bank or to any newly selected CSP.	
19.	The CSP/TSP should be able to adhere to the checklist issued by RBI Master Direction dated 10.04.23 on Outsourcing of Information Technology Services pertaining to "Usage of Cloud Computing Services"	
20.	The solution provided by the CSP/TSP shall be portable as well as interoperable to any other CSP (data export options needs to be considered in case bank require migration to another platform)	

Security Solutions in the Cloud

CSP must have the below Security Solution capabilities (an indicative list only) and the TSP should ensure enabling the below Security solutions wherever applicable in the cloud.

Sl.No	Security Solution		Compliance
1	Anti-DDOS		
1	WAF	Web Application Firewall	

2	SIEM	**Security Information and event management:** The CSP/TSP should establish a dedicated or managed SOC Team for ensuring security incident monitoring on 24x7 basis and effectively respond and remediate to security incidents.	
3	DAM	Database Activity Monitoring	
4	Antivirus Solution & EDR/XDR		
5	PIM (Privileged Identity Management)		
6	API Gateway		
7	Intrusion Prevention System (IPS), Intrusion Detection Solution (IDS), Host Intrusion Prevention System (HIPS)		

Certifications

The cloud service to be availed by the TSP for Bank shall at least have the following certifications, in addition to MEITY accreditation.

Mandatory certifications to consider	Compliance
ISO 27001 ISMS (Information Security Management System)	
ISO/CSF/DFSC 22301 certification (Security and resilience)	
PCI DSS (Applicable for storing/processing card transactions and payment information)	
SOC II Type 2	

Good to have/Preferable certifications to consider	Compliance
ISO 27017 (Cloud Security Management Certified)	
ISO/IEC 27018 (Personal Data in Cloud Certified)	
ISO/IEC 27701 PIM (Privacy Information Management) certified	
ISAE (International Standard on Assurance Engagements) 3402	

SOC III	
CSA Security Trust Assurance and Risk (STAR) Level 2 Certification	

We hereby comply with each point of the above Scope of Work without any deviations.

Signature with seal:
Name:
Designation:

Date

केनरा बैंक CANARA BANK Tender Processing Section C.P.V.M. Wing, H.O., Bengaluru

केनरा बैंक Canara Bank

Annexure-13
Bill of Material

SUB: RFP for Selection of Vendor for Implementation of Comprehensive Card-On-File Tokenization Solution for Generation of CoF Tokens for a Card in Canara Bank On OPEX Model for a Period of 3 Years

Ref: GEM/2024/B/5016455 dated 05/06/2024.

Notes

1. These details should be on the letterhead of Bidder and each & every page should be signed by an Authorized Signatory with Name and Seal of the Company.
2. The base location for the project execution would be Bangalore.
3. Please be guided by RFP terms, subsequent amendments and replies to pre-bid queries (if any) while quoting.
4. Do not change the structure of the format nor add any extra items.
5. No counter condition/assumption in response to commercial bid will be accepted. Bank has a right to reject such bid.
6. Applicable taxes will be paid on actuals.

Table -A
Implementation Cost for Card-On-File Tokenization Solution

[Amount in Rs.]

Sl. No.	Item Details	Price details (Excl. of Taxes)	Tax for Column a		Total Cost for Implementation (Incl. of Tax)
			% of Tax	Tax amt.	
		a	b	c	d=a+c
1	One Time Implementation Cost as per Scope of Work and Technical Requirements of the RFP				

Table -B
Cost for CoF Token

[Amount in Rs.]

Sl. No.	Item Details	Unit Price per token (Excl. of Tax)	Tax for Column a		Unit Price per token (Incl. of tax)	No of token per year *	No of Year	Total Cost For 3 years (Incl. of tax)
			% of tax	tax amt				
		a	b	c	d=a+c	e	f	g=dxexf
1.	CoF Token Cost					1,000,00	3	

* The quantity of token to be generated mentioned is indicative only and It may increase or Decrease as per the uses. Bidder has to provide the service at the rate quoted above during the entire contract period.

Table-C

Cost for any additional requirements /additional customization/ enhancement

[Amount in Indian Rupees]

Sl. No.	Description	Charges Per Man day (Excl. of Tax)	No. of man days per year#	No. of Years	Total Cost (Incl. of Tax)	Tax for column d		Total Cost (Incl. of Tax)
						% Tax	Tax amt.	
		a	b	c	d=(a*b*c)	e	f	g=d+f
1.	Cost for any additional requirements/ additional customization/ enhancement		100	3				

Number of man days mentioned above is indicative only. However, the no. of man days shall be as per actual utilization. The charges quoted above shall be fixed for the entire contract period.

Table-D

Total Cost for 3 Years Contract Period

[Amount in Indian Rupees]

Sl. No.	Details	Total Cost (inclusive of taxes)
1.	Total Implementation Cost as per Table-A	
2.	Total CoF Token Cost as per Table-B	
3.	Total Cost for any additional requirements/additional customization/enhancement as per Table-C	
4.	Total Cost of Ownership for a period of 3 years	

Undertaking

i. Bill of material is submitted on the letter head and is signed by an Authorized Signatory with Name and Seal of the Company.

ii. We confirm that we have gone through RFP clauses, subsequent amendments and replies to pre-bid queries (if any) and abide by the same.

iii. We have not changed the structure of the format nor added any extra items. We note that any such alternation will lead to rejection of Bid.

iv. We agree that no counter condition/assumption in response to commercial bid will be accepted by the Bank. Bank has a right to reject such bid.

v. We are agreeable to the payment schedule as per "Payment Terms" of the RFP.

vi. We confirm that there shall be no escalation in the agreed prices.

Date:

Signature with seal
Name:
Designation:

Annexure-14
Undertaking of Authenticity

(Should be submitted on Company's letter head with company seal and signature of the authorized person)

SUB: RFP for Selection of Vendor for Implementation of Comprehensive Card-On-File Tokenization Solution for Generation of CoF Tokens for a Card in Canara Bank On OPEX Model for a Period of 3 Years

Ref: GEM/2024/B/5016455 dated 05/06/2024.

We hereby undertake that all the hardware components/parts/assembly/software's used in this solution under the above like Servers, Switches, Hard Disk, Monitors, Memory etc., shall be original new components /parts /assembly /software only from respective OEMs/OSDs/OSOs of the products and that no refurbished / duplicate / second hand components / parts / assembly / software are being used or shall be used.

We also undertake that in respect of Licensed Operating System/Application Software/any other Software if asked for by you in the purchase order, the same shall be supplied along with the authorized license certificate (e.g. Product Keys on Certification of Authenticity in case of Microsoft Window Operating System/Software etc.) and also that it shall be sourced from the authorized source (e.g. Authorized Microsoft Channel in case of Microsoft Operating System).

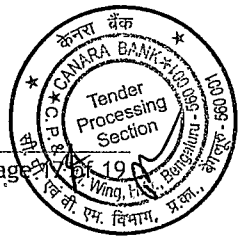
We confirm that the OS and software is free from bugs, malware, covert channels in code etc.

Should you require, we hereby undertake to produce the certificate from our OEM/OSD/OSO supplier in support of above undertaking at the time of delivery/installation. It will be our responsibility to produce such letters from our OEM/OSD/OSO supplier's at the time of delivery or within a reasonable time.

In case of default and we are unable to comply with the above at the time of delivery or during installation, for the IT Hardware/Software/Solution/Services already billed, we agree to take back the Hardware/Software/Solution/Services without demur, if already supplied and return the money if any paid to us by you in this regard.

Date:
Place:

Signature with seal
Name:
Designation:



केनरा बैंक Canara Bank

Annexure-15

Manufacturer Authorization Form

[Should be submitted on the letterhead of the OEM/OSO/OSD and signed by an Authorized Signatory of the OEM/OSO/OSD]

No._____ dated_____

The Deputy General Manager,
Canara Bank,
Centralized Procurement and Vendor Management Wing,
Naveen Complex, 14 M G Road,
Bengaluru - 560 001, Karnataka.

Dear Sir,

SUB: RFP for Selection of Vendor for Implementation of Comprehensive Card-On-File Tokenization Solution for Generation of CoF Tokens for a Card in Canara Bank On OPEX Model for a Period of 3 Years

Ref: GEM/2024/B/5016455 dated 05/06/2024.

We _____who are established and reputed manufacturers of _____having factories/development facilities at 1)_____and 2)_____do hereby authorize M/s_____(Name and address of the Agent/Dealer) to offer their quotation, negotiate and conclude the contract with you against the above invitation for GeM bid offer.

We (Manufacturer/Original Software Owner/Developer) hereby extend our full guarantee and warranty as per terms and conditions of the GeM bid and the contract for the solution, products/equipment and services offered against this invitation for GeM bid offer by the above firm and will extend technical support and updates and ensure availability of spares including processors for our products for contract period from the date of installation.

We (Manufacturer/Original Software Owner/Developer) also confirm that we will ensure all product updates (including management software updates and new product feature releases) are provided by M/s .....for all the products quoted for and supplied to the bank during the Contract period. In case this is not considered while quoting and in the event M/s ..... fail in their obligations to provide the updates within 30 days of release/announcement, we hereby confirm that we will provide the same to the bank at no additional cost to the bank and we will directly install the updates and any new Operating Software releases at the bank's premises.

We also confirm that the proposed solution offered by the bidder to the Bank are correct, viable, technically feasible for implementation and the solution will work without any hassles in all the locations. We also confirm that all the equipment offered are not "End of Life" during the next One Year and "End of Support" for total Contract Period.

We hereby commit to the GeM bid terms and conditions and will not withdraw our commitments during the process and or during the period of contract.

Yours faithfully
(Name)
For and on behalf of M/s

केनरा बैंक CANARA BANK Tender Processing Section C.P.V.M. Wing, H.O., Bengaluru - 560 001

केनरा बैंक Canara Bank

Annexure-16
Letter for EMD Return (if applicable)
[On Firm's / Company's letter head]

To
The Deputy General Manager,
Canara Bank,
Centralized Procurement and Vendor Management Wing,
Naveen Complex, 14 M G Road, Bengaluru-560 001.
Karnataka

Dear Sir,

SUB: RFP for Selection of Vendor for Implementation of Comprehensive Card-On-File Tokenization Solution for Generation of CoF Tokens for a Card in Canara Bank On OPEX Model for a Period of 3 Years

Ref: GEM/2024/B/5016455 dated 05/06/2024.

We _____ (Company Name) had participated in the Request for Proposal (RFP) for **Selection of Vendor for end to end implementation of Audit Solution in Bank for a Period of 5 Years**

Details of EMD submitted are as follows:

Sl. No.	Bidder Name	BG/DD/NEFT/RTGS Ref No.	Drawn on Bank Name	Date of BG/DD/NEFT/RTGS	Amount in Rupees

Bank details to which the EMD amount to be returned via NEFT/RTGS are as follows:

Account Title/Name	
Account Number	
IFSC Code	
Account Type	
Name of the Bank with Branch Address	

Declaration:

1. We here by note that the EMD submitted will be returned as per the terms and conditions of the RFP.

2. 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 Bank is not liable under any circumstances.

Date:
Place:

Signature with seal
Name:
Designation:

केनरा बैंक CANARA BANK Tender Processing Section 19 O. & M. Wing, Bengaluru - 560 001