Replies to Prebid queries to GeM Bid ref. no. GEM/2022/B/2431929 dated 12-08-2022 for Supply, Installation, Implementation, Configuration, Integration, Commissioning and Maintenance of PKI Software Solution for total period of 3 Years.

Sl. No.	Company Name	GeM Bid Clause	Clause/Technical Specification	Bidders Query	Bank's Reply
1	M/s. Odyssey Technologies Limited	ATC Annexure-1 Technical & Functional Requirement of PKI Software Solution	**1. Bank wants to engage a solution provider for implementing Public Key Infrastructure (PKI) solution for Internet Banking transactions with the following features:** e. PKI solution provider must ensure that certificates should not be stored in the terminal/PC. It should be securely stored in smart card/dongle in a non-exportable format.	In GeM a Category named 'PKI Software Solution' is un-available. The closest match for this phrase is in 'eSign with Embedded CA' category. This category allows only eSign Service Providers to participate. As per the technical specifications we understand that the bank wants an MFA solution with crypto token support. Please confirm if the purchaser is interested only for eSign based solution else there is a separate category named 'Multi Factor Authentication Software' for crypto token based transaction signing. We urge bank to create a bid in this category for the other sellers to participate.	Bidder to comply with the GeM bid terms as per the scope of work. .
2	M/s. Odyssey Technologies Limited	ATC Annexure-1 Technical & Functional Requirement of PKI Software Solution A. General Scope	**1. Bank wants to engage a solution provider for implementing Public Key Infrastructure (PKI) solution for Internet Banking transactions with the following features:** c. The solution should act as a multi-factor authentication (MFA) for performing Internet Banking transactions.	Please confirm other than DSC, is any other authentication factor expected by bank to authenticate / authorize their banking transactions	Bidder to comply with GeM bid terms.
3	M/s. Odyssey Technologies Limited	ATC Annexure-1 Technical & Functional Requirement of PKI Software Solution B. Components	3. Server Side Components to verify b. That the signature is mathematically valid and is of an acceptable format (PKCS#7/ CMS/XaDES, PaDES, JSON - credential management system).	The industry standard for signature storage are PKCS#7, CMS, XaDES, PaDES, CaDES, JSON. Considering the above standards please elaborate on what the clause 'Credential management system' refers to.	The GeM bid Clause is modified as under: 3. Server Side Components to verify b. That the signature is mathematically valid and is of an acceptable format (PKCS#7/ CMS/XaDES, PaDES, JSON)
4	M/s. Odyssey Technologies Limited	ATC Annexure-1 Technical & Functional Requirement of PKI Software Solution C. Features of the solution	d. The solution should be capable of supporting X.509 PKI certificates and should be able to use various security channels like PKCS#7, XML, OCSP, LDAP etc.	The standards mentioned here does not correlate with security channel specifications. The standards PKCS#7 - refers to signature packing / storage format, OCSP - refers to internet protocol for obtaining DSC status, LDAP - refers for directory service, ... So please amend the clause elaborating the security channels specifications expected	The GeM bid Clause is modified as under: d. The solution should be capable of supporting X.509 PKI certificates and should be able to use various security mechanisms like PKCS#7, XML, OCSP, LDAP etc., wherever required / applicable.
5	M/s. Odyssey Technologies Limited	ATC Annexure-1 Technical & Functional Requirement of PKI Software Solution C. Features of the solution	e. The solution should offer Digital Signing through USB Crypto Token or through e-sign which comply with CCA India guidelines.	We recommend the bank to amend the clause to use Crypto token based solution for signing banking transactions considering the following friction points: - High cost per transaction to Bank - Customer has to enter either Aadhaar number (or) Signer Id & PIN along with 2FA (OTP) for every transaction. Combining this with the existing login credentials results in additional client overheads. - Considering the bank wants to sign multiple transactions in a single request this is feasible only in a Non-Aadhaar based model (Signer ID & PIN). This increases the burden on customer since he has to undergo a tedious eKYC on-boarding process. Furthermore this process has to be repeated for every two years. - Likewise authentication in eSign service is done via OTP. This model is still vulnerable to all the shared secret attacks.	Bidder to comply with GeM bid terms.
6	M/s. Odyssey Technologies Limited	ATC Annexure-1 Technical & Functional Requirement of PKI Software Solution C. Features of the solution	k. The solution should have the ability to sign multiple transactions like Bulk Transactions at one time.		
7	M/s. Odyssey Technologies Limited	ATC Annexure-1 Technical & Functional Requirement of PKI Software Solution C. Features of the solution	i. The solution should be able to extract the public key from the transaction automatically for verification.	As per eSign CCA guidelines & API specifications provision for payload encryption is available only for Biometric data during Aadhaar based eSign transaction. Otherwise the channel is secured using TLS / SSL while the data is digitally signed and sent in plain. Any other changes to the eSign req-resp will violate the CCA specifications. Please confirm if the purchaser refers to the Biometric data encryption if not please elaborate the requirement	Bidder to comply with GeM bid terms.

8	M/s. Odyssey Technologies Limited	ATC Annexure-1 Technical & Functional Requirement of PKI Software Solution D. Administrator Dashboard and Alert module	e. The administrator shall be able to register, de-register or re-register and provide facilities like temporary block/unblock APIs for the customer certificates through the admin module.	Considering that the Bank has asked for API based model, the Internet banking application will integrate the APIs of the solution to consume Signing services of the solution. Hence the workflow design, GUI aesthetics is depedant on the Internet banking application rather than on the MFA solution. We urge bank to relax this clause else provide the necessary elaboration on what is the expectation for this clause.	Bidder to comply with GeM bid terms.
9	M/s. Odyssey Technologies Limited	ATC Annexure-1 Technical & Functional Requirement of PKI Software Solution D. Administrator Dashboard and Alert module	f. Solution should support workflow templates that allows for user friendly customer registration and should have maker-checker mechanism for workflow approval through an admin console.		Bidder to comply with GeM bid terms.
10	M/s. Odyssey Technologies Limited	ATC Annexure-1 Technical & Functional Requirement of PKI Software Solution H. Performance	a. Solution should be able to handle '200 to 300' number of concurrent transactions/validations across multiple channels.	To offer the optimal hardware sizing we request bank the provide the folloing volumetric details : Number of Business Applications for authorizing transactions using DSC Approx number of Users to be enrolled for 3 years Number of signing transactions performed in day / month / Year Payload size of the transactions (for storage) Please confirm the maximum Transaction Per Second expected is 300 TPS.	The relevant details will be shared with the selected bidders
11	M/s. Odyssey Technologies Limited	ATC Annexure-1 Technical & Functional Requirement of PKI Software Solution H. Performance	b. Solution shall be able to enrol unlimited users without any users restrictions	To offer the optimal hardware sizing we request bank the provide the folloing volumetric details : Number of Business Applications for authorizing transactions using DSC Approx number of Users to be enrolled for 3 years Number of signing transactions performed in day / month / Year Payload size of the transactions (for storage) Please confirm the maximum Transaction Per Second expected is 300 TPS.	The relevant details will be shared with the selected bidders
12	M/s. Odyssey Technologies Limited	ATC Annexure-1 Technical & Functional Requirement of PKI Software Solution H. Performance	c. Solution shall be able to migrate/verify the existing digitally signed transactions already completed using existing application.	Please clarify a. Whether the exisiting customer use a DSC crypto token b. The details of the exisiting digitally signed transactions, like - Signature storage format - Whether the signature is stored in attached or dettached model - Necessary CRL / OCSP verification information embedded in the signature - Database storage schema / structure	Bidder to comply with GeM bid terms.
13	M/s. Odyssey Technologies Limited	Additional terms and conditions 8. Delivery, Installation, Integration and Commissioning	8.2. The proposed services will be hosted in Canara Bank premises (DC & DR).	Considering that the bank is open to eSign Service can the bidder propose *'Authentication As a Service'* based solution. It offers - Payload encryption feature - Compartmentallization of individual business applications / instances - Sign anytime / anywhere, use crypto tokens in Smartphones too - Miltrary grade security, truly protects users from MITM, Phishing, SIM swaps, key loggers, Trojans - Zero learning curve for users - No more client end overheads like installation of Controls / Java / change system settings, etc.	Bidder to comply with GeM bid terms.
14	M/s. Odyssey Technologies Limited	Generic	Generic	Considering that time required to process the pre-bid clarifications, collate and submit the bid documents we request the bank to extend the bid submission by another week.	Bidder to comply with GeM bid terms.
15	M/s. Odyssey Technologies Limited	Generic	Item Category PKI Software Solution (Q3)	In GeM a Category named 'PKI Software Solution' is un-available. The closest match for this phrase is in 'eSign with Embedded CA' category. This category allows only eSign Service Providers to participate. As per the technical specifications we understand that the bank wants an MFA solution with crypto token support. Please confirm if the purchaser is interested only for eSign based solution else there is a separate category named 'Multi Factor Authentication Software' for crypto token based transaction signing. We urge bank to create a bid in this category for the other sellers to participate.	Bidder to comply with GeM bid terms.

16	M/s. Unibrain Consultancy Service Private Limited (Software Development company)	Generic	Assumption regarding Bank Transactions:	1. It is assumed that the Bank will share all the transaction details where Digital Signing functionality needs to be incorporated. 2. It is assumed that the Bank will share customer details for DSC capture/mapping. 3. It is assumed that changes required in the Banking software for accommodating digital signature will be addressed by the Banking Software team. 4. It is assumed that the technology/software architecture details of the Banking software that is required for PKI implementation will be shared	Bidder to comply with GeM bid terms.
17	M/s. Unibrain Consultancy Service Private Limited (Software Development company)	Generic	Generic	PKI functionality on Mac can be supported if certificate is stored in the Mac's Key Store; otherwise, it is dependent on the certificate storage device provider and their driver software.	Bidder to comply with GeM bid terms. The solution should support MAC OS also.

Date: 30/08/2022
Place: Bangalore

Deputy General Manager