Minutes of the Pre-Bid Meeting

Tender No. GEM/2025/B/6527169

Description of the service: Hiring of services for Multi Factor Authentication (MFA) for 03 years.

Date & Time: 18.08.2025 at 9:00 A.M.

Venue: IT Conference Hall, IT Department, OIL FHQ, Duliajan, Assam - 786602.

The pre-bid meeting was organized to address the queries raised by the bidders for the said tender within the pre-bid query submission deadline. OIL discussed and clarified the queries pointwise. The queries received & clarifications given, if any during the meeting are enclosed as **Annexure –I**. It was mentioned in the meeting that the final reply against each pre-bid query shall be published in the GeM portal and the same will be treated as part of the tender conditions and shall be binding to both OIL and Bidders.

The meeting ended with a vote of thanks to the chair.

Bidders from the following firms joined the pre-bid meeting offline/online through VC:

1. Sonata Information Technology Limited. (online)
2. Commercial Friends. (offline)
3. Embee Software Pvt. Ltd. (online)

OIL's Representative		Bidder's Representative		
Sr. No.	Signature, Name, Designation & date	Sr. No.	Signature, Name, Designation & date	Firm's Name
1	SOURABH KR. BORCHETIA, DGM(IT)	1		
2	MANAS JYOTI BORDOLOI CE-IT	2		
3	MIGANG MIGOM PEGU CE-IT	3		
4	RACKTIM BHUYAN, CE-IT	4		
5	KRISHNARCHAN P. BORAH EMCO[MCCS]	5		
6		6		

Annexure-I

	M/s. Commercial Friends (Physically present)	
Sl. No.	**Query**	**OIL's Response**
1	The proposed 2FA solution must support secure user authentication by implementing a two-factor mechanism and must incorporate location based access control capabilities. The system should evaluate the user's geographic location during the authentication process and enforce predefined access policies accordingly.	Shall be reviewed
2	The proposed 2FA solution must distinguish between managed and unmanaged endpoints/devices & should allow access to corporate applications from managed devices/endpoints	Shall be reviewed
3	The proposed Two-Factor Authentication (2FA) solution must support device health checks as part of the authentication flow. It should assess the security posture of endpoints—including Windows, macOS, Linux, and Chrome browser-based access (via enterprise-managed Chrome profiles)—and enforce access policies based on configurable health requirements. Health check such as firewall enabled, system password set, disk encryption enabled, BitLocker enabled should be supported. In case Linux is not supported, third party tool should be integrated to provide the asked capabilities.	Shall be reviewed
4	The proposed Two-Factor Authentication (2FA) solution must include secure and configurable “Remember Device” functionality to improve user experience while maintaining strong security controls. This feature should allow trusted devices to bypass repeated 2FA prompts for a specified period—both for browser-based applications and for Windows login (desktop authentication)—without compromising security or compliance requirements.	Shall be reviewed
5	The proposed Two-Factor Authentication (2FA) solution must include the ability to evaluate Operating system of Android, Windows, MAC etc. during authentication attempts from devices. The system must allow administrators to define policies that block access from outdated/vulnerable Android, windows and Mac, chrome OS versions. The solution should also provide notification to end-user to update their device OS as part of a secure authentication process.	Shall be reviewed
6	The proposed 2FA solution should provide the following to make sure 2FA used is secure and easy to use by the end user : i. The solution should provide the capability to configure passwordless authentication ii. Should have multiple phishing resistant MFA with proximity push that verifies the access device and the user are together. iii. Quickly enable workers to strongly authenticate once per day across any browser or thick client without session cookies. iv. Desktop SSO should support thick clients, embedded browsers and cross-browser sessions. v. Obtain Wi-Fi fingerprint location information and use it for risk-based authentication. vi. It must have a function to control access according to the global IP based location of the device.	Shall be reviewed
7	The proposed Two-Factor Authentication (2FA) solution must allow administrators to identify and control access based on the browser type such as Firefox, safari, chrome, edge, IE, chrome mobile, Firefox mobile, mobile safari, edge chromium mobile used during authentication attempts.	Shall be reviewed
8	The 2FA solution must be capable of detecting the browser type used during the authentication process and must provide user-facing warnings if the browser is out of date or no longer supported. The system should allow administrators to define what qualifies as “outdated” and configure policies for enforcement or guidance.	Shall be reviewed
9	The 2FA solution must support conditional access policies that allow users to bypass 2FA when accessing from trusted network locations.	Shall be reviewed
10	The proposed Two-Factor Authentication (2FA) solution should enforce 2FA for login attempts originating from anonymous or high-risk networks, including public VPNs, Tor exit nodes, proxies & anonymizers	Shall be reviewed

Annexure-I

M/s. Sonata Information Technology Limited (attended through VC)

Sr. No.	Document	Page No	Category	RFP Clause	Query	OIL's Response
1	1754120416-PQC	1	1.1 TECHNICAL EVALUATION CRITERIA:	1.1.1 Experience Criteria: Bidder must have successfully completed/executed at least one SIMILAR WORK of value not less than Rs. 15,49,600.00 (Rupees Fifteen Lakh Forty-Nine Thousand Six Hundred) over the last 07 (Seven) years reckoned from the original bid closing date in Central or State PSUs / Central or State Government Organization / Public Limited / Nationalised Banks Company in India.	Please change to "Experience Criteria: Bidder must have successfully completed/executed at least one SIMILAR WORK of value not less than Rs. 15,49,600.00 (Rupees Fifteen Lakh Forty-Nine Thousand Six Hundred) over the last 07 (Seven) years reckoned from the original bid closing date in Central or State PSUs / Central or State Government Organization / Public Limited / Nationalised Banks/ Enterprise Company in India."	No change
2	1754120420-Payment Terms	1	1.0 PAYMENTS TERMS:	1.2 Payment against license charge for 300 users (item no. 10) and support service charge (item no. 30) shall be paid on quarterly basis.	Kindly change to "Payment against license charge for 300 users (item no. 10) and support service charge (item no. 30) shall be paid on yearly basis."	No change
3	1754120420-Payment Terms	1	1.0 PAYMENTS TERMS:	1.3 Payment against license charge for additional 300 users (item no. 20) will be paid on actuals on quarterly basis.	Please change to"Payment against license charge for additional 300 users (item no. 20) will be paid on actuals on yearly basis."	No change

Annexure-I

M/s. Embee Software Pvt. Ltd. (attended through VC)

Section No.	Clause No. (Page No.)	Tender specification	request for change	Suggestion	OIL's Response
1.2 (B) - Security	clause - (i) , pg - no 1 in SOW document	Authentication App shall display information about authentication request like application, location of use, time zone information of access device.	The application details are required in the authentication App & information like location of use, time zone information of access device to be available in administration console .	The availability of location of use, time zone information of access device in the administration console can help in policy decision and monitoring abnormal user activity & should be integrated with SOC tool like SIEM for corelation. Availability of information in authentication app for Normal users wont be of any help in interpreting or apprehending any suspicious login activity.	Shall be reviewed
1.2 -c- Administration	clause-(ii) , pg - no 2 in SOW document	The MFA service shall support admins to enrol and provision users via a) an E-mail b) link sent via SMS.	Activities like user enrolment & provisioning are critical activities & secure mechanism like Email should only be allowed.	User enrolment and provising by SMS based mechanism are not secure & are prone for theft via various mechanism & should not be supported.	Shall be reviewed
1.3 24x7 SOLUTION SUPPORT	vii) Support Channels , pg no 4 in SOW document	a) The service provider must offer multiple support channels for incident resolution. b) 24x7 Dedicated Support Portal for ticket management. c) Toll-Free Helpdesk Number for immediate assistance. d) Email Support with a guaranteed response time. e) Live Chat Support for quick troubleshooting.	Request that these service management mechanisms are available with bidder for better service life cycle management and outcome.	the mentioned channel availability with bidder would ensure that the service practise of the bidder is mature & better service outcome can be expected.	No change
1.1 TECHNICAL EVALUATION CRITERIA	1.1.1 Experience Criteria , pg no 1 in PQC document	Bidder must have successfully completed/executed at least one SIMILAR WORK of value not less than Rs. 15,49,600.00	As the tender in question is for MFA service , kindly specify that the supplied product with asked value should be also be accompanied with separate managed service order for the delivered item in PO copy produced in compliance to this clause.	This would allow bidders with service capabilities and experience.	Shall be reviewed

Annexure-I

M/s. InstaSafe Technologies Pvt. Ltd. (did not attend the pre-bid meeting)

Sl. No.	Query	OIL's Response
1	With reference to the GeM Tender No. GEM/2025/B/6527169 dated 02.08.2025 for "Custom Bid for Services - Hiring of services for Multi Factor Authentication (MFA) for 03 years", we would like to submit our intent to participate in the bidding with our MII Class 1 certified solution. InstaSafe Technologies Pvt. Ltd. is a leading Indian cybersecurity company headquartered in Bengaluru. We have been serving enterprise and government customers across India for over a decade, with a strong focus on Zero Trust Network Access (ZTNA), Identity and Access Management (IAM), and Multi-Factor Authentication (MFA) solutions. Our products are entirely designed, developed, and supported in India, and are fully compliant with Make in India (MII) and Aatmanirbhar Bharat initiatives. We have noted that the tender terms currently specify that the purchase preference for MII is not applicable. Considering the Government of India's emphasis on promoting indigenous solutions under the Make in India program, this comes as a surprise. It may be pertinent to highlight that several similar MFA tenders issued by Government PSUs have included MII purchase preference clauses. In fact, many leading PSUs such as GAIL, Indian Oil, PGCIL, NHPC, LIC, NIC and CDAC have incorporated MII Class 1 purchase preference in their recent MFA and cybersecurity tenders. For your ready reference, we are also enclosing copies of such tenders where MII preference has been duly recognized. We respectfully request your kind consideration to amend the tender conditions to include MII purchase preference, in line with national policy and to ensure equitable opportunities for indigenous products.	No change as deliberated in the pre-bid meeting

Annexure-I

M/s. CCS Computers Pvt. Ltd. (did not attend the pre-bid meeting)

Sl. No.	Section	Point	Query	Suggestion	OIL's Response
1	1.2 TECHNICAL REQUIREMENTS: A) General Requirements:	1.2 A(1)(d) Authentication via Phone Call	Is there any specific used case for delivering OTPs via phone call, considering that it may not be secure? Would it be more beneficial to explore alternative, more secure methods?	We suggest keeping this point as optional if this is not mandatory or not needed for current requirement	No change