Addendum - RFP - Multifactor Authentication Solution

Please refer to the **RFP** published on the ReBIT's website on January 16, 2020 inviting submission of bids from eligible vendors for providing professional services for **Multifactor Authentication Solution**, an Addendum containing the following changes to the above RFP document has been released Addendum.

Addendum

Sr. No.	Terms & Conditions/Section given in the RFP	Added / Changed as
1	3.1: Schedule (Page 7)	Revised RFP dates for bidders.
2	10.16: Annexure P: Commercial Bid Format (Page 75)	Revised the commercial bid format
3	10:18: Annexure R: Technical Specifications	Added the Technical Specifications in RFP

- **3.1: Schedule (Page 7)**
  - Revised RFP dates for bidders.

Activity	Scheduled Dates
Name of Project	Multifactor Authentication Solution (MFA)
Issue of RFP	28-January-2020
Last date and time for receipt of mail queries for clarification from Bidders	04-Febuary-2020 by 04:00 pm
Date and time of Pre-Bid Meeting (including existing system overview)	11-Febuary-2020

Venue for Pre-Bid Meeting	(at ReBIT office meeting time to be communicated to interested bidder via email)
Last date to publish Meeting-cum-Addendum to the bid document	18-Febuary-2020
Date & Time of Final Submission of Technical & Commercial Bids.	21-Febuary-2020 02:00 PM
Date and Time of Technical Bid Opening	21-Febuary-2020 04:00 PM
Technical Bid Presentation by the Bidders Before the Committee	To be communicated
Commercial Bid Opening	To be communicated
Declaration of Final Result	To be communicated
All Queries to be mailed to	procurement@rebit.org.in

- **10.16: Annexure P: Commercial Bid Format (Page 75)**
  - Revised the commercial bid format

		Warranty			AMC	
Point No.	**0**	**Year 1 (A)**	**Year 2 (B)**	**Year 3 (C)**	**Year 4 (D)**	**Year 5 (E)**
1	Hardware Cost (Server) + OS	Yes	Included in Year 1		AMC Cost	AMC Cost
2	Application/Software/subscription Cost for 50 Users	Yes	Yes	Yes	Yes	Yes
3	Implementation Cost (Please Provide The Cost Details)	Yes, (This Should be part of Year 1 (subscription Cost))	Not Required			
4	Training Cost	Yes	Not Required			
5	Support Cost (365*24*7) (Hardware + OS + Software)	Yes, (This Should be part of Year 1 (subscription Cost))	Yes, (This Should be part of Year 2 (subscription Cost))	Yes, (This Should be part of Year 3 (subscription Cost))	Yes, (This Should be part of Year 4 (subscription Cost))	Yes, (This Should be part of Year 5 (subscription Cost))
	TOTAL	Year 1 Total (Point 1+2+4)	Year 2 Total (Point 2)	Year 3 Total (Point 2)	Year 4 Total (Point 1+2)	Year 5 Total (Point 1+2)
	TCO	(A+B+C+D+E)				
	Incremental Licenses / Subscription cost					
	Application/Software/subscription Cost for 100 Users	YES	YES	YES	YES	YES
	Application/Software/subscription Cost for 200 Users	YES	YES	YES	YES	YES
	Application/Software/subscription Cost for 200 + Users	YES	YES	YES	YES	YES

- **10:18: Annexure R: Technical Specifications**
  - Added the Technical Specifications in RFP

Please Refer the “RFP - Technical_Specification_MFA”

ReBIT - Multifactor Authentication Solution Specification - Capacity						
Sr. No.	Details	Requirement specification	Requirement categorisation	Total Marks	Compliance (Y/N)	Detailed response (please be as elaborate as possible on how your solution addresses these points)
1	General Functionalities	The proposed solution should be able to provide multifactor authentication for Windows, Mac, Linux Operating systems & Database etc.	Must Have	5		
2		The proposed solution be able to provide multifactor authentication for VPNs, Firewall, Network Switch's, Router, Wireless controllers and web proxy	Must Have	5		
3		The proposed solution should provide multifactor authentication for emails (server & end users)	Must Have	5		
4		The proposed solution should provide multifactor authentication for in-house developed application	Must Have	5		
5		The proposed solution should provide multifactor authentication for cloud service providers like Azure, AWS, cloud SaaS solutions Office 365.	Must Have	5		
6		The proposed solution should be able to customise the Time-Based One-Time Password (TOTP) frequency	Must Have	5		
7		The proposed solution should provide multifactor authentication for virtualization platform (HCI)	Must Have	5		
8		The proposed solution should be on premise deployment.	Must Have	5		
9		The proposed solution should have single console for management, configuration, and monitoring.	Must Have	5		
10		The proposed solution should provide automated audit and access logs, reports for any access violation.	Must Have	5		
11		The proposed solution should have manageability over web applicaition console using HTTPS protocol	Must Have	5		
12		The bidder should provide SSL certificate wherever required.	Good to Have	3		
13		The solution should support Android, IOS for soft token.	Must Have	5		
14		The solution should support integration with MAM solution.	Must Have	5		
15		The proposed solution should support user self-servicing and password management functionality to allow users to manage their own registrations and passwords without administrator intervention	Must Have	5		
16		The proposed solution should provide Soft Token (TOTP)/Hardware Token/Push Notification/Email	Must Have	5		
17		The proposed solution should provide custom reports like based on GEO location, Access Type, Time etc.	Must Have	5		
18		The proposed solution should provide strong emergency login mechanism during solution malfunction	Must Have	5		
19		The proposed solution should be able to integrate with LDAP solution for user authentcation	Must Have	5		
20		The proposed solution not store any users credentials on database	Must Have	5		
21		The proposed solution should provide authentication at protocol level	Must Have	5		
22		The proposed solution should be able to provide the original IP and geo location of the user making the access request	Must Have	5		
23		The proposed solution should be able to disable/Wipe the soft token remotely in case of any security incidents.	Must Have	5		
24		The proposed solution should provide proprietary mobile app for IOS, Andriod	Must Have	5		
25		The proposed solution should have inbuilt two factor authentication for accessing MFA admin console	Must Have	5		
26		The proposed solution should be able to deploy agents remotely	Good to Have	3		
27		The proposed solution should should support thin client	Good to Have	3		
28		The proposed solution should support Adaptive / Risk based authentication capabilities.	Good to Have	3		
29		The proposed solution should support hard tokens from other OEM as long as they are OATH compliant with 5- 7 years of lifetime.	Must Have	5		
30		The proposed solution should support both Open ID and SAML 2.0 natively and should be able to integrate with ADFS.	Must Have	5		
31		The proposed solution should support failover to the authentication server at the DR site when the authentication server at primary site goes down.	Must Have	5		
32		The proposed solution should be able to integrate with third party applications such as reverse proxy solution, and PIM solution.	Must Have	5		
33		The proposed solution should offer APIs to either extend or customize the application.	Good to Have	3		
34		The proposed solution should be able to be deployed in virtual environments such as VMware, LPAR or Hyper-V	Must Have	5		
35		The solution should support database storage on SAN (storage area network)	Good to Have	3		
36		The Solution should have Inbuilt Reporting for Secure Access, Successful/Failed Authentication, System Reports and other authentication Reports.	Must Have	5		
37		Information for all policies, groups, and roles should be stored in the LDAP repository or, alternatively, in a database.	Must Have	5		
38		The system should allow the administrators to create temporary policies and apply these policies to temporary subset of users in order to validate the settings applied.	Must Have	5		
39		The Authentication Mechanism should provide capabilities to prevent Brute Force Attacks and should be able to send alerts to the Admin/Helpdesk in case of a brute force attack on a user account.	Must Have	5		
40	Performance, Scalability and Availability	Minimum utilization of system resources on endpoints i.e system resources used by the agent has to be below 10% and the memory utilization should be within 200 MB.	Must Have	5		
41		Minimum utilization of network bandwidth while authentication client should not utilize bandwidth more than 1 Mbps.	Must Have	5		
42		The agent should be dormant/idle when not performing any authentication activities.	Must Have	5		
43		The server infrastructure should be horizontally scalable; additional infrastructure/hardware can be added to support higher usage and high availability including DR	Good to Have	3		
44		The proposed solution should provide embedded database	Must Have	5		
45	Pre-Requisites and Dependencies	The proposed solution should not have any conflict with existing infrastructure security solutions.	Good to Have	3		
46		The solution agent size should be less than 100 MB.	Must Have	5		
47	Strength of Security	Industry grade (AES-256) encryption should be used for data flow between Central server and clients	Must Have	5		
48		The communication between central server and client endpoints irrespective of their location should be secured with encryption	Must Have	5		
49	Administration	Administrator should be able to create customized dashboard to view compliance status and history.	Must Have	5		
50		Administrator should be able to view current client status in detail.	Must Have	5		
51		Administrator must be able to generate all type of reports in pdf, csv and excel format.	Must Have	5		
52		Administrator should be able to configure email to send weekly compliance reports.	Must Have	5		
53		Administrator must be:able to define role-based access to the various function areas of the solution and restrict user role including, but not limited to, administration, reporting, event filtering, correlation, and /or dashboard viewing.	Must Have	5		
54		The proposed solution should have Backup and Restoration of all policies and database.	Must Have	5		
55		Client agent should have anti tamper password. (requires additional credential to uninstall)	Must Have	5		
56	Integration	Integration with SIEM to analyze and parse security events/logs generated.	Must Have	5		
57		Integration with Active Directory to import OU & Groups for administration task and management	Must Have	5		
58		Integration with mail server for email alerts for 2FA and it should send reports	Must Have	5		
59	Hardware Token	The proposed solution should have 8-character high contrast LCD display with pin padded H/W token.	Good to Have	3		
60		The proposed solution should have OATH compliant time based	Good to Have	3		
61		The proposed hardware endurance more than 14,000 clicks	Good to Have	3		
62		The proposed hardware should have Battery life cycle more than 5 years	Good to Have	3		
63		The proposed solution should have OATH TOTP Compliant RoHS CE FCC WEEE	Good to Have	3		
64		The proposed solution should have fingerprint enabled option for authentication.	Good to Have	3		
			Total Score	**292**		