WEBEL TECHNOLOGY LIMITED

CORRIGENDUM – 1

WTL/PAR/AUA-ASA/22-23/054 dated 30.03.2023

Sl. No.	Section No.	Page/Clause No.	Clause Description	Clarification / Revised clause
1	SECTION-B: Eligibility Criteria	Page-50,Clause no.4	The bidder must have prior experience of successfully implementation of at least **two projects** on Aadhaar Authentication framework implementation and maintenance of Aadhaar AUA / KUA functionality as well as expertise/technical skill set in setting up ASA/KSA in last three years as on Bid submission date	Pleased read as " The **bidder/ Group Company** must have prior experience of successfully implementation of at least **one projects** on Aadhaar Authentication framework implementation and maintenance of Aadhaar AUA / KUA (Aadhaar stack include HSM,ADV,AUA/KUA stack, e-KYC middleware) in last three years as on Bid submission date. Bidder should have expertise/technical skill set in setting up ASA/KSA".
2	SECTION-B: Eligibility Criteria	Page-51,Clause no.9	**Past Experience**: a. The bidder should have experience in successfully implementation & roll-out of Aadhar Authentication Framework through setting up AUA/ KUA including onboarding of multiple Sub-AUA applications through development of API, experience in design, development of proven Aadhaar Data Vault, e-KYC middleware and all associated software stack as per UIDAI guidelines and security framework including its Operation & Maintenance and AMC support to the satisfaction of client as well as experience/skill set in setting up ASA/KSA with integration with UIDAI CIDR Database for at least two (2) organizations in India (Central Government/State Government/PSU/Private Sector Company). Out of the above, at least one ADV development and implemented AUA/KUA, should be operational over a period of at least 1 year.	Please read as : **Past Experience:** a. The **bidder/ Group Company** should have experience in successfully implementation & roll-out of Aadhar Authentication Framework through setting up AUA/ KUA(Aadhaar stack include HSM,ADV,AUA/KUA stack, e-KYC middleware) including onboarding of multiple Sub-AUA applications through development of API, deployment of proven Aadhaar Data Vault, e-KYC middleware and all associated software stack operational for at least one year as per UIDAI guidelines and security framework including its Operation & Maintenance and AMC support to the satisfaction of client as well as technical skill set in setting up ASA/KSA with integration with UIDAI CIDR Database for at least **one organizations** in India (Central Government/State Government/PSU/Private Sector Company**/Banking, Insurance, BFSI**).

			b. The bidder must have carried out at least 10 Cr transactions on AUA/KUA platform, during last two years. c. The bidder must have carried out at least 50,000 e-Sign transactions during last one year	b. The **bidder/Group Company** must have carried out at least 10 Cr Aadhar Transaction (Authentication as Yes/No/e-KYC transactions) on AUA/KUA platform during last two years.
3	SECTION-B: Eligibility Criteria	Page-52,Clause no.10	The bidder should be ISO 9001:2015,ISO 27001:2013 and CMMi Level 3 or higher Certificate. The certificate should be valid as on the date of submission of the bid and the bidder should ensure that valid certification is maintained throughout the period of implementation of the project.	Please read as "The bidder should be ISO 9001:2015,ISO 27001:2013. The certificate should be valid as on the date of submission of the bid and the bidder should ensure that valid certification is maintained throughout the period of implementation of the project"
4	SECTION-1	Page-12 sl no 1.4	**1.4 Application Programming Interfaces (APIs)** PKCS#11 Open SSL Java (JCE) Microsoft CAPI and CNG Third Party Payment API SDK to support Java PHP and other Scripting languages ✓ Memory within HSM (MB) 32 or more ✓ Number of Partitions within HSM minimum 5 field programmable and scalable to higher capacity partitioning ✓ 1 or more Supported Cryptographic Algorithm (Asymmetric) RSA (2048-8192) RSA (2048-4096) ✓ Key Storage Area All keys within FIPS Boundary In HSM As per UIDAI Circular	**Please read as:** **1.4 Application Programming Interfaces (APIs)** PKCS#11 Open SSL Java (JCE) Microsoft CAPI and CNG Third Party Payment API SDK to support Java PHP and other Scripting languages ✓ Memory within HSM (MB) 8 or more ✓ Number of Partitions within HSM at least 20 partitions ✓ HSM should have at least 10,000 keys ✓ 1 or more Supported Cryptographic Algorithm (Asymmetric) RSA (2048-8192) RSA (2048-4096) ✓ Key Storage Area All keys within FIPS Boundary In HSM As per UIDAI Circular
5	SECTION-1	Page-12 sl no 1.5	**1.5 Signing Speed RSA 2048 Bit** (Transactions per second) 1000 or more Signing Speed Supported Cryptographic Algorithm (Symmetric) Published as additional Specifications parameters AES 3DESIf Inside HSM Key Storage Capacity for triple DES Published as additional Specifications parameters 40000If Inside HSM Key Storage Capacity for RSA 2048 Bit Published as additional Specifications parameters 20000If Inside	This clause is deleted

			HSM Key Storage Capacity for AES 128-256 Published as additional Specifications parameters 40000Form Factor 19 " Rack Mountable 1U or 2U	
6	SECTION-I	Page-17 sl no 1.11(6)	Same HSM and ADV would be scaled to multiple Govt Departments under same Government through provisioning of partitioning within the HSM with data gets separated because of partitioning with encryption keys and tokenization keys for each department under separate partition. Bidder must ensure HSM with Higher Partition (at-least 20 partition capable of field programmable upto100 partition) in the HSM to meet the above purpose. ADV for each of the department will have separate encryption keys for tokenization)	Please read as : Same HSM and ADV would be scaled to multiple Govt Departments under same Government through provisioning of partitioning within the HSM with data gets separated because of partitioning with encryption keys and tokenization keys for each department under separate partition. Bidder must ensure HSM with Higher Partition (**at-least 20 partitions**) in the HSM to meet the above purpose. ADV for each of the department will have separate encryption keys for tokenization.
7	SECTION-I	Page-91 sl no 1.1 (17)	Support for minimum 1000 Transaction per Second @ RSA 2048 bits field programmable to higher capacity TPS	Support for minimum 1000 Transaction per Second @ RSA 2048 bits field
8	SECTION-I	Page-91 sl no 1.1 (13)	Storage capacity of cryptographic memory should be field upgradable to 10000 RSA Keys of 2048 bits with license upgrade	Storage capacity of cryptographic memory should have at least 10000 RSA Keys of 2048 bits
9	SECTION-I	Page-91 sl no 1.1 (11)	Minimum keys storage should be 5000 RSA keys of 2048 bits within FIPS 140-2 Level 3 certified crypto memory only (storage on NVRam not allowed)	Minimum keys storage should be 10000 RSA keys of 2048 bits within FIPS 140-2 Level 3 certified crypto memory only (storage on NVRam not allowed)
10	SECTION-I	Page-91 sl no 1.1 (19)	HSM should have at least 5 logical user partition scalable to 100 without any additional cost involvement , each user partition should have its own Username and PIN	HSM should have at least 20 logical user partition, each user partition should have its own Username and PIN
11	SECTION-I	Page-91 sl no 1.1 (18)	HSM should be field upgradable to higher TPS and higher key storage	This clause is deleted

12	SECTION-I	Page-12 sl no 1.2.3(2)	Secure key storage storing of the encryption / decryption keys protected by a FIPS and CC EAL 4+ certified HSM device and restricting direct access to the keys	Please read as: Secure key storage storing of the encryption / decryption keys protected by a FIPS 140-2 Level-3 and CC EAL 4+ certified HSM device and restricting direct access to the keys. **Certification should be in the name of proposed OEM only.** Certification copy needs to be submitted (FIPS 140-2 certification on Third Party OEM will not be considered)
13	SECTION-I	Page-96 sl no 9	HSM should be of 1000 TPS @ RSA 2048 bits field programmable to higher capacity TPS and 1 GBPS - Encryption / decryption	Please read as: HSM should be of 1000 TPS @ RSA 2048 bits and 1 GBPS - Encryption / decryption and 1GBPS is the network port speed of the HSM
14	SECTION-I	Page-95 sl no 10.5	Support for many types of rates limiting capabilities including rate limits by request counts and network bandwidth usage	Please read as: The proposed software solutions of the bidder should have deployment of Open source API Gateway to Support for many types of rates limiting capabilities including rate limits by request counts and network bandwidth usage
15	SECTION-I	Page-95 sl no 10.6	Ability to assign quotas to user, application , IP addresses , devices and regions among other things	Please read as: The proposed software solutions of the bidder should have deployment of Open source API Gateway to ensure Ability to assign quotas to user, application , IP addresses , devices and regions among other things
16	SECTION-I	Page-95 sl no. 12.3	Support for Security audit by UIDAI security consultant or organization appointed consultant	Please read as: The bidder is to provide security audit through Cert-in empaneled auditors and the cost involvement shall be borne by the bidder.
17	SECTION-I	Page-96 sl no. 11	The software should be able to tokenize numeric / alpha numeric and special character other than Aadhar numbers in its current version	Please read as: The software should be able to tokenize numeric value. It can encrypt other PII data
18	SECTION-I	Page-96 sl no. 17	User access should be locked in case of 5 unsuccessful login attempts. Audit log of all the activities carried out in Aadhar data vault should be maintained as per the policies mandated by UIDAI.	Please read as : User access should be locked in case of 5 unsuccessful login attempts. Audit log of all the activities carried out in Aadhar data vault should be maintained as per the policies mandated by UIDAI. Email Gateway (using WB.GOV.IN

				Mail Server) and SMS Gateway will be provided by P&AR Depart to send alerts
19	SECTION-1	Page-97 sl no. 22	The solution should be able to support file level encryption in transparent manner. No downtime is expected while data is transformed into encrypted data(HSM speed of 1GBPS AES encryption decryption is considered)	This clause is deleted
20	SECTION-1	Page-41,clause-17.1(4), Page-43,clause 17.3(4) Page-44,clause-17.5(4) Page-45,clause-17.6(4), Page-46,clause-17.9(4), Page-47,clause-17.11(4)	Network Interface per physical Server- – Dual port 25 Gig Ethernet Card populated with 2 nos. of 25GbE SFP28 Multimode transceivers and – 4 nos. of Multimode Patch Cords of minimum 3m length – 1 no. of 1GbE dedicated management interface. (Direct Attached Cables should not be proposed to meet the transceiver requirement).	Please read as: Network Interface per physical Server- – Dual port 25 Gig Ethernet Card populated with 2 nos. of **10/25GbE** SFP28 Multimode transceivers **supporting dual speed auto-negotiating** and – 4 nos. of Multimode Patch Cords of minimum 3m length – 1 no. of 1GbE dedicated management interface. (Direct Attached Cables should not be proposed to meet the transceiver requirement).
21	SECTION-1	Page 48, clause 17.13	Ports : 28 x SFP+ ports with transceivers 2 x QSFP28 ports supporting 10 / 25 / 40 / 50 / 100 GbE ports	Please read as : Ports : 28 x **10G** SFP+ ports with transceivers 2 x QSFP28 ports supporting 10 / 25 / 40 / 50 / 100 GbE ports
22	SECTION-1	Page 48, clause 17.13(6)	Protocols & services- QoS, ACL, OSPF, BGP and PBR. Converged network support for Data Center Bridging, with priority flow control (802.1Qbb), ETS (802.1Qaz), DCBx and iSCSI TLV	Please read as : Protocols & services- QoS, ACL, OSPF, BGP and PBR. Converged network support for Data Center Bridging, with priority flow control (802.1Qbb), ETS (802.1Qaz)/ DCBx
23	SECTION-1	Page 39, clause 16 B(5)-MySQL Tool	Server-1	Please read as : Server-2

24	SECTION-1	Page 10, clause 1.3.1	Supply, install and maintain the Hardware Security Module (HSM) at the locations specified WB State Data Center (SDC as Primary Site)& Disaster Recovery(DR)) at Purulia, West Bengal. DR site is not ready right now	Please read as: Supply, install and maintain the Hardware Security Module (HSM) at the locations specified WB State Data Center (SDC as Primary Site)& Disaster Recovery(DR)) at Purulia, West Bengal. DR site is ready
25	Annexure-1	Page-124, clause (9)	Volume of e-Sign transactions carried out during last year. Number of transactions : 50000 to 1 lakh for 3 marks 1 to 5 lakhs for 4 marks >=5 lakhs for 5 marks Maximum marks 5	Volume of e-KYC transactions carried out on AUA/KUA platform during last year. 10 – 11 Crores : 3 marks 11-15 crores : 4 marks >15 crores : 5 marks Maximum marks 5
26	SECTION-1	Page-41,clause-17.1(1), Page-42,clause 17.3(1) Page-43,clause-17.5(1) Page-45,clause-17.7(1), Page-46,clause-17.9(1), Page-47,clause-17.11(1)	Physical Cores- minimum 2 x 24 Cores (3rd/4th Generation Intel Xeon processor minimum 2.0 GHz speed).	Please read as: Physical Cores-minimum 2 x 24 Cores (3rd/4th Generation Intel Xeon processor /AMD EPYC processor minimum 2.4 GHz speed).
27	Annexure-1	Page-123, clause (3)	The bidder should have experience in successfully implementation & roll-out of Aadhaar Authentication Framework through setting up AUA/ KUA including onboarding of multiple Sub-AUA applications through development of API, experience in design, development & widely proven Aadhaar Data Vault, e-KYC middleware and all associated software stack as per UIDAI guidelines and	Please read as :The Bidder/Group Company should have experience in successfully implementation & roll-out of Aadhaar Authentication Framework through setting up AUA/ KUA including onboarding of multiple Sub-AUA applications through development of API, experience in deployment of widely proven Aadhaar Data Vault, e-KYC middleware and all associated software stack

			security framework including its Operation & Maintenance and AMC support to the satisfaction of client for at least two (2) organizations in India (Central Government/State Government /PSU /Private Sector Company) each of which value more than Rs 2 Crore. Out of the above, at least one ADV development and implemented AUA/KUA, should be operational over a period of at least 2 years.	as per UIDAI guidelines and security framework including its Operation & Maintenance and AMC support to the satisfaction of client for at least one organizations in India (Central Government/State Government /PSU /Private Sector Company/Banks.Insurance,BFSI) each of which value more than Rs 2 Crore.
28	Annexure-1	Page-124, clause (4)	The Bidder should have the experience of successfully implementing Aadhaar Authentication Projects and have authenticated at least 30 Crore Aadhaar numbers for any Govt Department in India	The Bidder/Group Company should have the experience of successfully implementing Aadhaar Authentication Projects and have authenticated at least 30 Crore Aadhaar numbers for any Govt Department in India
29	Annexure-1	Page-124, clause (5)	The Bidder should have the experience of successfully implementing Aadhar Authentication Projects and have integrated at least 5 AUA/Sub-AUAs/Schemes for any Govt. Department in India	The Bidder/Group Company should have the experience of successfully implementing Aadhar Authentication Projects and have integrated at least 5 AUA/Sub-AUAs/Schemes for any Govt. Department in India
30	SECTION-1	Page-23	Software development for Reengineering Cloud	This clause is deleted
31	SECTION-1	Page-42,clause-17.2(2), Page-43,clause 17.4(2) Page-44,clause-17.6(2) Page-46,clause-17.8(2), Page-47,clause-17.10(2),	OEM support for 5 (five) years for proposed cloud, virtualization, security software, operating system, database software etc.	Please read as : OEM support for 5 (five) years for proposed virtualization, security software, operating system, database software etc.

		Page-48,clause-17.12(2)		
32	New clause			Offered software solution by the bidder must include **Fraud Monitoring System** as per UIDAI guidelines without any additional cost involvement
33	New clause			Offered software solution by the bidder must include capability to monitor suspicious transactions, location bound transactions, unauthorized transactions etc as best as possible