

IDRBT Clarifications to the pre-bid queries on Tender No: IDRBT/SYS/VR/120/2022 – 2023 dated 10th August, 2022 for Supply, Installation and Maintenance of Hardware Security Modules (Network based & PCIe Card based) at IDRBT

Sr.No.	RFP Section Number	RFP Page Number	RFP Point Number	Query Description	Comment / Suggestion / Deviation	IDRBT Comments/Clarifications
1	5. Bidders Eligibility Criteria	8	S.No. 2. Duration of past experience	The Bidder should have experience in the following fields: Supply, Installation and Maintenance of Hardware Security Modules (Network based & PCIe Card based) for the organizations across India	Please revise experience criteria "The Bidder should have experience in : Supply, Installation and Maintenance of Hardware Security Modules Network based or PCIe Card based for the organizations across India	"The Bidder should have experience in : Supply, Installation and Maintenance of Hardware Security Modules Network based and / or PCIe Card based for the organizations across India
2	5. Bidders Eligibility Criteria	8	S.No. 5 Technical Capability	Bidder must have successfully completed in the last three years at least the following numbers of similar IT infrastructure (HSM) Implementation engagement(s) of value specified herein: <ul style="list-style-type: none"> • One project of similar nature not less than the amount Rs.1 Crore OR • Two projects of similar nature not less than the amount equal Rs.60 Lakhs OR • Three projects of similar nature not less than the amount equal Rs.50 Lakhs 	Please remove this clause. As exemption for MSME	No Change. The procurement and services provided by the System Integrator are critical in nature.
3	5. Bidders Eligibility Criteria	8	S.No. 8 Support	Bidder should have a local entity in Hyderabad to provide better support during the warranty and AMC period.		No Change
4	6. Terms & Conditions	6	6.6 of Terms & Conditions	The Supply, Installation of Hardware Security Modules (Network based & PCIe Card based) at IDRBT should be completed within 8 (Eight) weeks from the date of issue of purchase order	Please revise to "The Supply, Installation of Hardware Security Modules (Network based & PCIe Card based) at IDRBT should be completed within 16 weeks from the date of issue of purchase order.	Accepted, "The Supply, Installation of Hardware Security Modules (Network based and / or PCIe Card based) at IDRBT should be completed within 16 weeks from the date of issue of purchase order.
5	10. Delivery & Installation Period	10	Point a. Delivery ≤ 6 Weeks	The following time schedule for completion of the activities from the date of placement of orders should be strictly adhered to Point a. Delivery ≤ 6 Weeks	Please revise Point a. Delivery ≤ 16 Weeks	Clarified above at Sr.No 4
6	23. Payment Terms	17	23.2. 10 percent (10%) PBG	Performance Bank Guarantee for an amount being 10% of the Contract Price, would be payable after successful warranty period is over from the date of acceptance or payable against PBG valid as per warranty period	Please remove this clause	No Change

IDRBT Clarifications to the pre-bid queries on Tender No: IDRBT/SYS/VR/120/2022 – 2023 dated 10th August, 2022 for Supply, Installation and Maintenance of Hardware Security Modules (Network based & PCIe Card based) at IDRBT

Sr.No.	RFP Section Number	RFP Page Number	RFP Point Number	Query Description	Comment / Suggestion / Deviation	IDRBT Comments/Clarifications
7	Network HSM Specifications - A.Technical Specifications	30	2	The HSM should be FIPS 140-2 level 3 and CC EAL 4+ certified modules, such certifications should be under the name of OEM supplying the HSM to IDRBT. All IDRBT keys including Private Keys should be stored and protected within Certified memory HSM device for entire key life cycle.	CC EAL4+ certification is been asked, however at all other place in specification only FIPS 140-2 Level 3 certification is been referred. Also as we see in below points CCA IVG guidelines is referred, CCA IVG guidelines only asks for FIPS 140-2 Level 3 certification. CCA has never asked for CC EAL4+ certification, so we request you to please remove CC EAL4+ certification. IDRBT has specifically asked for FIPS 140-2 Level 3 certification in name of OEM. In earlier RFP IDRBT has always asked for FIPS 140-2 Level 3 Compliance, never referred about certification in name of OEM. It seems to be suggested by some vendor to eliminate Make in India HSM from this bid. We would request to keep it as previous RFP's where Cryptographic keys need to be stored in FIPS 140-2 Level 3 Certified Cryptographic Module. "If keys are stored in FIPS 140-2 level 3 certified Cryptographic Module , then it fully complies with CCA guidelines"	Optional. However, the bidder should be able to provide CC EAL 4+ certified modules as and when advised by CCA Guidelines, on no obligation basis to IDRBT.
8	Network HSM Specifications - B. Cryptographic Algorithm Support	31	3	The HSM device should support for Hash Message Digest HMAC, SHA1, SHA2 (512) and SM3 etc.,	SM3 is chinese Algorithm , request to please remove same	Accepted.
9	Network HSM Specifications - B. Cryptographic Algorithm Support	31	4	The HSM device should support various cryptographic algorithms like Asymmetric Key RSA (1024-4096 bits), DSA , (ECDSA, ECDH,Ed25519, ECIES) and KCDSA etc.,	KCDSA is korean algorithm , request to please remove same	Accepted.
10	Network HSM Specifications - B. Cryptographic Algorithm Support	31	5	The HSM device should support BIP32 algo for Wallet encryption.	BIP32 is Bitcoin Improvement Proposal algorithm, which is not under FIPS/NIST approved list. Request you to please remove same. Also IDRBT being RBI governed entity, would not be promoting Bitcoin infrastructure	Accepted.
11	Network HSM Specifications - C. Other Specifications	31	6	The successful bidder should use the existing Backup HSM and seamlessly migrate the keys from the existing HSM device to the newly proposed HSM. The existing applications should seamlessly work with the new HSM.	Migration of keys from existing HSM to new HSM is ok, but why existing backup HSM need to be used? Secondly migration of keys from existing HSM to new HSM, assumption is existing HSM would be able to export keys outside HSM.	The bidder may use Backup device/Network HSM device. However, the Key migration from existing HSM to New HSM should be safe, secure and as per CCA guidelines. The existing applications should seamlessly work with the new HSM.
12	Network HSM Specifications - C. Other Specifications	31	9	The bidder should quote Network HSM, backup device and accessories with 1-year warranty, and 4 Year additional warranty on Network HSM, backup device and accessories.	Existing backup device need to be used is been mentioned above point. This point ask for new backup device.	Yes, the bidders should quote for new Backup device, PED device and necessary cables etc.,

IDRBT Clarifications to the pre-bid queries on Tender No: IDRBT/SYS/VR/120/2022 – 2023 dated 10th August, 2022 for Supply, Installation and Maintenance of Hardware Security Modules (Network based & PCIe Card based) at IDRBT

Sr.No.	RFP Section Number	RFP Page Number	RFP Point Number	Query Description	Comment / Suggestion / Deviation	IDRBT Comments/Clarifications
13	Network HSM Specifications - C. Other Specifications	31	10	The HSM device should support Safety & Environmental Compliance like UL,CSA,CE ; FCC,CE,VCCI,C-TICK,KC Mark ; RoHS2, WEEE	For Safety and Environmental compliance India has come up with BIS certification, however here all international certification is been asked. Would request you to please keep only BIS certification as this procurement is within India.	Accepted.The HSM device should support Safety & Environmental Compliance like BIS,UL,CSA,CE ; FCC,CE,VCCI,C-TICK,KC Mark ; RoHS2, WEEE
14	Technical Specifications for PCIe Card based HSM- A.General Specifications		1	The Hardware security module should be a PCIe card based and compatible with popular server hardware models.	We understand this particular device is used for offline CA or Root CA, We have network appliance HSM particularly developed for Offline CA and Root CA requirements. So we request you to please allow to quote Network Appliance HSM for this requirement of yours.	Not accepted.
15	Technical Specifications for PCIe Card based HSM- A.General Specifications	32	3	The HSM should be FIPS 140-2 level 3 and CC EAL 4+ certified modules, such certifications should be under the name of OEM supplying the HSM to IDRBT. All IDRBT keys including Private Keys should be stored and protected within Certified memory of HSM device for entire key life cycle.	CC EAL4+ certification is been asked, however at all other place in specification only FIPS 140-2 Level 3 certification is been referred. Also as we see in below points CCA IVG guidelines is referred, CCA IVG guidelines only asks for FIPS 140-2 Level 3 certification. CCA has never asked for CC EAL4+ certification, so we request you to please remove CC EAL4+ certification. IDRBT has specifically asked for FIPS 140-2 Level 3 certification in name of OEM. In earlier RFP IDRBT has always asked for FIPS 140-2 Level 3 Compliance, never referred about certification in name of OEM. It seems to be suggested by some vendor to eliminate Make in India HSM from this bid. We would request to keep it as previous RFP's where Cryptographic keys need to be stored in FIPS 140-2 Level 3 Certified Cryptographic Module. "If keys are stored in FIPS 140-2 level 3 certified Cryptographic Module , then it fully complies with CCA guidelines"	Clarified above at Sr.No 7
16	Technical Specifications for PCIe Card based HSM- A.General Specifications	32	6	The required HSM must support PCI-Express CEM 3.0, PCI, PCI Express Base 2.0	Please allow to quote Network Appliance HSM also for this requirement, as we have built specific device to replace PCI-express device and give customer option to their specification with other specially designed network appliance HSM	Clarified above at Sr.No 14
17	Technical Specifications for PCIe Card based HSM- B.Cryptographic Algorithm and Support	32	3	The HSM device should support Hash Message Digest HMAC, SHA1, SHA2 (512) and SM3	SM3 is chinese Algorithm , request to please remove same	Clarified above at Sr.No 8
18	Technical Specifications for PCIe Card based HSM- B.Cryptographic Algorithm and Support	32	4	The HSM device should support various cryptographic algorithms like Asymmetric Key RSA (1024-4096 bits), DSA , (ECDSA, ECDH, Ed25519, ECIES) and KCDSA etc.,	KCDSA is korean algorithm , request to please remove same	Clarified above at Sr.No 9

IDRBT Clarifications to the pre-bid queries on Tender No: IDRBT/SYS/VR/120/2022 – 2023 dated 10th August, 2022 for Supply, Installation and Maintenance of Hardware Security Modules (Network based & PCIe Card based) at IDRBT

Sr.No.	RFP Section Number	RFP Page Number	RFP Point Number	Query Description	Comment / Suggestion / Deviation	IDRBT Comments/Clarifications
19	Technical Specifications for PCIe Card based HSM-B.Cryptographic Algorithm and Support	33	5	The HSM device should support BIP32 algo for Wallet encryption.	BIP32 is Bitcoin Improvement Proposal algorithm, which is not under FIPS/NIST approved list. Request you to please remove same. Also IDRBT being RBI governed entity, would not be promoting Bitcoin infrastructure	Clarified above at Sr.No 10
20	Technical Specifications for PCIe Card based HSM-C.Other Specifications	33	7	The successful bidder should use the existing Backup HSM and seamlessly migrate the keys from the existing HSM device to the newly proposed HSM. The existing applications should seamlessly work with the new HSM.	Migration of keys from existing HSM to new HSM is ok, but why existing backup HSM need to be used? Secondly migration of keys from existing HSM to new HSM, assumption is existing HSM would be able to export keys outside HSM.	Clarified above at Sr.No 11
21	Technical Specifications for PCIe Card based HSM-C.Other Specifications	33	8	The device should not have root or super-user access to HSM appliance in any way like No access to bash , ksh or any default terminal shells etc.,	This point do not point valid as its PCI Card	Noted.
22	Technical Specifications for PCIe Card based HSM-C.Other Specifications	33	10	The bidder should quote PCIe Card HSM, backup device and accessories with 1-year warranty, and 4 Year additional warranty on PCIe Card HSM, backup device and accessories.	Existing backup device need to be used is been mentioned above point. This point ask for new backup device.	Yes, the bidders should quote for new Backup device, PED device and necessary cables etc.,
23	Technical Specifications for PCIe Card based HSM-C.Other Specifications	33	11	The HSM device should support Safety & Environmental Compliance like UL,CSA,CE ; FCC,CE,VCCI,C-TICK,KC Mark ; RoHS2, WEEE	For Safety and Environmental compliance India has come up with BIS certification, however here all international certification is been asked. Would request you to please keep only BIS certification as this procurement is within India.	Clarified above at Sr.No 13
24	23. Payment Terms	14	23.2. 10 percent (10%) PBG	Performance Bank Guarantee for an amount being 10% of the Contract Price, would be payable after successful warranty period is over from the date of acceptance or payable against PBG valid as per warranty period	Please remove PBG clause	Clarified above at Sr.No 6
25	5. Bidders Eligibility Criteria	5	S.No. 2. Duration of past experience	The Bidder should have experience in the following fields: Supply, Installation and Maintenance of Hardware Security Modules (Network based & PCIe Card based) for the organizations across India	Please revise experience criteria "The Bidder should have experience in : Supply, Installation and Maintenance of Hardware Security Modules Network based or PCIe Card based for the organizations across India	Clarified above at Sr.No 1
26	5. Bidders Eligibility Criteria	5	S.No. 5 Technical Capability	Bidder must have successfully completed in the last three years at least the following numbers of similar IT infrastructure (HSM) Implementation engagement(s) of value specified herein: • One project of similar nature not less than the amount Rs.1 Crore OR • Two projects of similar nature not less than the amount equal Rs.60 Lakhs OR • Three projects of similar nature not less than the amount equal Rs.50 Lakhs	Please remove this clause.	Bidder must have successfully completed in the last three years at least the following numbers of similar IT infrastructure (HSM) Implementation engagement(s) of value specified herein: • One project of similar nature not less than the amount Rs.1 Crore OR • One projects of similar nature not less than the amount equal Rs.60 Lakhs OR • Two projects of similar nature not less than the amount equal Rs.50 Lakhs

IDRBT Clarifications to the pre-bid queries on Tender No: IDRBT/SYS/VR/120/2022 – 2023 dated 10th August, 2022 for Supply, Installation and Maintenance of Hardware Security Modules (Network based & PCIe Card based) at IDRBT

Sr.No.	RFP Section Number	RFP Page Number	RFP Point Number	Query Description	Comment / Suggestion / Deviation	IDRBT Comments/Clarifications
27	6. Terms & Conditions	6	6.6 of Terms & Conditions	The Supply, Installation of Hardware Security Modules (Network based & PCIe Card based) at IDRBT should be completed within 8 (Eight) weeks from the date of issue of purchase order	Please revise to "The Supply, Installation of Hardware Security Modules (Network based & PCIe Card based) at IDRBT should be completed within 15 weeks from the date of issue of purchase order". Reason is global supply of hardware delayed from OEMs hence it is taking longer time for delivery.	Clarified above at Sr.No 4
28	10. Delivery & Installation Period	10	Point a. Delivery ≤ 6 Weeks	The following time schedule for completion of the activities from the date of placement of orders should be strictly adhered to Point a. Delivery ≤ 6 Weeks	Please revise Point a. Delivery ≤ 15 Weeks	Clarified above at Sr.No 4
29	13. Penalty for Delay	11	13.Penalty for Delay	For any delay in installation and commissioning of the equipment beyond the specific period, IDRBT will charge penalty @ 0.5% of the order per week or part thereof, subject to a maximum of 6%.	Please remove this clause.	Not accepted.
30	25. Order Cancellation		25. Order Cancellation	IDRBT reserves its right to cancel the order in the event of delay in delivery and installation beyond the stipulated time.	Please remove this clause.	Not accepted.
31	9. Scope of Work	13	16.b	The successful bidder shall ensure that faults and failures intimated by IDRBT as above are set right within 24 hours of being informed of the same.	Resolution period for the issue depends on multiple unknown factors, however response time to troubleshoot will be within 2 hours for critical issues.	Accepted.
32	12. System maintenance, Support and Preventive maintenance	14	12.2	The successful bidder shall ensure that faults and failures intimated by IDRBT as above are set right within 24 hours of being informed of the same.	Resolution period for the issue depends on multiple unknown factors, however response time to troubleshoot will be within 2 hours for critical issues.	Accepted.
33	14. Penalty for downtime	14	14	Any equipment viz (Network HSM / PCIe Card HSM) that is reported to be down should be either fully repaired or replaced by temporary substitute (of equivalent configuration) within 1 working days.	In case of the hardware failure and confirmation of RMA, the replacement will be shipped by the OEM in the next business day.	Accepted.
34	16. Training	15	16.1	A Comprehensive training shall be the key to successful Operations and Maintenance; hence, the successful bidder is required to provide training (for three days) to IDRBT nominated Officials at IDRBT, Hyderabad.	Please modify the training period to 1 day and mode of delivering the training through Virtual means.	Section 16.1 is updated as "A Comprehensive training shall be the key to successful Operations and Maintenance; hence, the successful bidder is required to provide training (for three days) to IDRBT nominated Officials either in virtual mode or physical mode, at least one day should be in physical mode at IDRBT, Hyderabad."
35	2. Objective of the project	2	2. Objective of the project	Description : 1. Network based Hardware Security Module Type II, 2. PCIe Card based Hardware Security Module Type I	Please explain Type-1 and Type-2 mentioned in description	2. Objective of the project Table Description Sr.No 1 Read as "Network based Hardware Security Module" and Sr.No 2 Read as "PCIe Card based Hardware Security Module".

IDRBT Clarifications to the pre-bid queries on Tender No: IDRBT/SYS/VR/120/2022 – 2023 dated 10th August, 2022 for Supply, Installation and Maintenance of Hardware Security Modules (Network based & PCIe Card based) at IDRBT

Sr.No.	RFP Section Number	RFP Page Number	RFP Point Number	Query Description	Comment / Suggestion / Deviation	IDRBT Comments/Clarifications
36	9. Scope of Work	12	9. Scope of Work : Point no 7	The successful bidder to ensure that OEM should also provide certificate that all Equipment's offered are not be declared End of Life and End of Support for a minimum of 7 years from the date of acceptance	Please revise to "The successful bidder to ensure that OEM should also provide certificate that all Equipment's offered are not be declared End of Life and End of Support for a minimum of 5 years from the date of acceptance"	Accepted
37	18. Period of Validity	13	18. Period of Validity	All the prices and other terms and conditions of the offer proposed by the bidder should be Valid for a minimum period of Six months	Please revise to "All the prices and other terms and conditions of the offer proposed by the bidder should be Valid for a period of One month"	Not accepted.
38	Annexure – IX	30	HSM Specifications. Point no 1	The HSM should support a minimum of 100 Transaction Signing per Second for RSA 2048 bits	Please revise to "The HSM should support a minimum of 100 Transaction Signing per Second for RSA 2048 bits" Reason is existing HSM with IDRBT itself has 350 TPS. Keeping in view additional applications integration with HSM in Future we recommend minimum 1000 TPS	Not accepted.
39	Annexure – X	32	HSM Specifications. Point no 2	The HSM should support a minimum of 100 Transaction Signing per Second for RSA 2048 bits	Please revise to "The HSM should support a minimum of 100 Transaction Signing per Second for RSA 2048 bits" Reason is existing HSM with IDRBT itself has 350 TPS. Keeping in view additional applications integration with HSM in Future we recommend minimum 1000 TPS	Not accepted.
40	Annexure – X	33	C. Other Specifications. Point no 7	The successful bidder should use the existing Backup HSM and seamlessly migrate the keys from the existing HSM device to the newly proposed HSM. The existing applications should seamlessly work with the new HSM.	Please revise to "The successful bidder should use the existing Backup HSM and 'PED devices' and seamlessly migrate the keys from the existing HSM device to the newly proposed HSM. The existing applications should seamlessly work with the new HSM"	Clarified above at Sr.No 11
41	Annexure – XII	35	Network HSM Devices, Description no 1	Network HSM backup device and accessories, with 1 year warranty.	Please revise to "Network HSM and accessories, with 1 year warranty."	In Commercial Bid format Annexure XII Sr.No 1 Read as "Network HSM device, Backup device and accessories, with 1 year warranty."
42	Annexure – XII	35	HSM PCIe Cards, Description no 4	HSM PCIe Card backup device and accessories, with 1 year warranty.	Please revise to "HSM PCIe Card and accessories, with 1 year warranty."	In Commercial Bid format Annexure XII Sr.No 4 Read as "HSM PCIe Card, Backup device and accessories, with 1 year warranty."
43		5	Technical Capability	Bidder must have successfully completed in the last three years at least the following numbers of similar IT infrastructure (HSM) Implementation engagement(s) of value specified herein: <ul style="list-style-type: none"> • One project of similar nature not less than the amount Rs.1 Crore OR • Two projects of similar nature not less than the amount equal Rs.60 Lakhs OR • Three projects of similar nature not less than the amount equal Rs.50 Lakhs 	We request amendment from Two Projects done by bidder of 60 lacs to One Project done above 60 lacs	Clarified above at Sr.No 26
44	Bid Schedule	7	Last date for receipt of Bidding Documents	30th August 2022 3:30 PM		6th September 2022 3:30 PM