

Corrigendum to Tender No: IDRBT/SYS/AKT/145/2025 – 2026 dated 31st July 2025

MSTC No :: IDRBT/Head Office/Procurement/7/25-26/ET/7[HSM PED Backup HSM] dated 31st July 2025

Request for Proposal (RFP) For Supply, Installation and Maintenance of Hardware Security Modules (Network based), PED and HSM Backup devices at IDRBT locations

Clarifications to Pre-Bid meeting held on 8th August 2025 at 15:00 Hrs with the bidders at IDRBT, Hyderabad, following amendments to the RFP document are made with immediate effect. Responses to pre-bid meeting are uploaded on MSTC Portal and IDRBT Web site separately,

No Change in bid Schedule.

Contact details

i.	All Queries to be mailed to	itprocurement@idrbt.ac.in
ii.	MTSC Portal for bid submission.	https://www.mstcecommerce.com/eprocn/

Sr. No	RFP Section No.	RFP Page No.	RFP Point No.	RFP Description	Query Description	IDRBT Response
1	Annexure – IX(a)	42	7	"The HSM should be FIPS 140-2 level 3 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."	Request to modify the clause as:- The HSM should be FIPS 140-3 level 3 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	<i>Clause stand revised to also reflect FIPS 140-3 Level 3 certification, subject to OEM certification validity and assurance of backward compatibility with existing FIPS 140-2 infrastructure.</i>
2	Annexure – IX(a)	43	12	"HSM RNG should comply with AIS 20/31 to DRG.4 using HW based true noise source alongside NIST 800-90A NIST 800-90B, NIST 800-90C compliant CTR-DRBG"	Random Number Generation "Using HW based true noise source" is a vendor-specific clause, Request to modify the clause as :- Random Number Generation: should be designed to comply with AIS 20/31 to DRG.4 and compliant to NIST 800-90A/800-90B, CTR-DRBG or hash based random number generator.	Clause stand revised to allow hash-based RNGs, provided compliance with AIS 20/31 and NIST 800-90A/B standards.
3	Annexure – IX(a)	44	22	"The device should support GUI administration, management and maintenance of partitions like creating, modification, reading, deletion of partitions remotely without access to physical device."	Request to modify the clause as :- "The device should support GUI/CLI administration, management and maintenance of partitions like creating, modification, reading, deletion of partitions remotely without access to physical device."	<i>No Change. CLI may be additional feature.</i>
4	Annexure – IX(a)	51	3	"Shall maintain compatibility with at least two major HSM OEMs without proprietary locks"	Request to remove this clause	<i>Condition removed</i>

Sr. No	RFP Section No.	RFP Page No.	RFP Point No.	RFP Description	Query Description	IDRBT Response
5	-	20	8	Delivery 2 weeks and implementation 1 week .	Request modification :Delivery - 3-4 weeks and implementation 4-5 weeks	<i>Delivery revised to 3 weeks, Implementation to 1 week.</i>
6	6. Scope of Work	15	Point5 - iii	"A requirement for the bidder to simulate a full DR failover test post-installation and annually thereafter."	Is the DR failover simulation to be conducted at both DC and DR sites or consolidated in one site?	<i>As in RFP</i>
7	6. Scope of Work	15	Point 7	"Real-time health monitoring of HSMs, PEDs, and Backup HSMs via SNMP/REST APIs"	Are there any existing SNMP or REST-based monitoring tools in use?	<i>As in RFP</i>
8	6. Scope of Work	16	Point 10 – vi	"If the OEM's Network HSM does not support the existing PEDs or Backup HSMs, the bidder must supply compatible PEDs that: <ul style="list-style-type: none"> · Are backward-compatible with the existing Network and PCIe HSMs. · Support seamless key migration and backup/restore operations. · Do not disrupt existing cryptographic workflows or compliance requirements" 	Can you confirm the exact make/model and firmware versions of the existing PEDs and Backup HSMs that need to be supported?	<i>As in RFP</i>
9	6. Scope of Work	16	Point 10 - x	Bidders to submit a detailed migration strategy including wrapped key formats, PED compatibility, rollback plan	Is the key format and wrapping method used in the existing HSMs available for review and compatibility validation?	<i>As in RFP</i>

Sr. No	RFP Section No.	RFP Page No.	RFP Point No.	RFP Description	Query Description	IDRBT Response
10	6. Scope of Work	17	Point 10 – xiii	"The bidder shall implement a comprehensive cryptographic key lifecycle management policy covering key generation, activation, rotation, archival, and secure destruction. All key lifecycle operations must be logged, auditable, and compliant with FIPS 140-2 Level 3 and CCA IVG guidelines. Automated key rotation and expiry enforcement must be configurable per partition."	a- Does IDRBT currently use any centralized key management solution, or is the bidder expected to provide and configure such a platform as part of the solution? b- Please clarify the format, retention period, and integration requirements (e.g., SIEM, syslog) for audit logs generated during key lifecycle operations.	<i>Separate line item in technical price(for process) and price bid may be submitted.</i>
11	23	26	23.2	10 percent (10%) would be payable after successful warranty period is over from the date of acceptance or payable against PBG valid as per warranty period.	Please clarify the PBG value or percentage	<i>PBG shall be 10% of contract value, valid for warranty duration.</i>
12	2.1	12	8	Support Bidder should have a local entity in Hyderabad to provide better support during the warranty period.	Please clarify what kind of documentary evidence need to submit here	<i>Certificate of Incorporation, GST Registration, or Lease Agreement showing local entity presence in Hyderabad.</i>
13	Technical Annexure -iX(a)	Page No. 43	Point No. 16	HSM supports the capability to run the custom code inside the HSM.	What type of custom code you are referring ?	<i>As in RFP</i>
14	Technical Annexure -iX(a)	Page No. 49	Point No. 25	"Compatibility Matrix" showing support for existing APIs and SDKs	Please provide firmware version of your existing PED devices.	<i>As in RFP</i>
15	2.1. Bidder Eligibility Criteria	Page No. 10	Point No. 02	The Bidder should have experience in the following fields: Supply, Installation and Maintenance of Hardware Security Modules (Network based) for the organizations across India. The Bidder should submit documentary evidence in support of minimum experience of 3 years	Request to accept experience of implementing and managing the same kind of infrastructure with a global client outside of India.	<i>As in RFP</i>