Technical Specification & Compliance

SL No	Name of Item	Description	Compliance & Bidder Response (Y/N)
1	Brand	Mentioned by the bidder	
2	Model	Network HSM (Model to be specified by OEM)	
3	Quantity	Total Requirement is: **03 (Three)**	
4	Partitions	Minimum 5 (five) partitions, each partition should be active from Day-01.	
5	Cryptographic interfaces	Full Suite B support • Asymmetric: RSA, DSA, Diffie-Hellman, Elliptic Curve Cryptography (ECDSA, ECDH, Ed25519, ECIES) with named, user-defined and Brain pool curves, KCDSA, and more. • Symmetric: AES, AES-GCM, Triple DES, DES etc. • Hash/Message Digest/HMAC: SHA-1, SHA-2, SHA-3, SM2, SM3, SM4 and more • Key Derivation: SP800-108 Counter Mode • Key Wrapping: SP800-38F	
6	Supported Operating Systems	Windows, Linux. Virtual: VMware, Hyper-V, Xen, KVM.	
7	API Support	PKCS#11, Java (JCA/JCE), BouncyCastle API's should be supported REST API for administration. Should support Customized and Validated Firmware and API for BACH II	
8	Partitions	Should support partitioning of FIPS 140-2 certified HSM memory into completely isolated divisions and not just logical partitioning in associated software with each partition managed by their own Security Officer and Crypto Officer Roles and having independent security policies that can be managed. From Day one 5 partition for each HSM will be activate. For High Availability (HA) each device should support at least two partitions for BACH II and two for NIKASH (Prod. & UAT)	
9	Security Certifications	• FIPS 140-2 Level 3 • Qualified Signature or Seal Creation Device (QSCD) listing for eIDAS compliance.	
10	Performance Capacity	Signing performance of 1000 TPS for RSA 2048	
11	Authentication Method	Must have FIPS 140-2 Level 2 Password based	
12	Host Interface	Min. 4 x 1G with Port Bonding	
13	Physical Characteristics	Standard 1U 19in. rack mount appliance	

SL No	Name of Item	Description	Compliance & Bidder Response (Y/N)
14	Safety & Environmental Compliance	• UL, CSA, CE • FCC, CE, VCCI, C-TICK, KC Mark • RoHS2, WEEE • TAA • BIS [IS 13252 (Part 1)/IEC 60950-1]	
15	Reliability	• Dual hot-swap power supplies • Field-serviceable components • Mean Time Between Failure (MTBF) at least 170000 Hours	
16	Management & Monitoring	• HA disaster recovery. • SNMP & Syslog • ----------	
17	Backup	Vendor should shear procedure and accessories (if require) to take backup of HSM, especially configuration, partition schemas, certificates etc. The backup should be restorable and recoverable from offline device or designated components to another (supplied) HSM	
18	Key Migration	Provided HSM should support Key Migration from existing HSM model in a FIPS 140-2 compliant manner without the keys coming out in clear for BACH	
19	Warranty	3 years warranty with 24x7 Telephonic and Email provided directly from OEM	
20	Installation, Testing and Commissioning	Bidder must carry out on site installation, testing and commissioning. Bidder must configure appropriate security and administration related policies. Bidder has to provide all kind of accessories including patch cord to establish all kind of connections	
21	OEM Confirmation	Awardees vendor will have to submit authorized MAF from OEM on the network HSM for BACH-II project & Nikash	
22	BB Confirmation	HSM Should support BACH (officially approved by Bangladesh Bank), Nikash & IDTP Platform	
22	Local Partner Support	Dedicated 24/7 support team of OEM and local partner presence in Bangladesh with certified resources, as well as should have RMA material in Dhaka	
23	Training	Awardee vendors have to arrange a training session on overview of the HSM for 4 (four) banks personnel.	
24	Load balancing capability	HSM must support load balancing & Auto Failover capability without any external load balancer	

SL No	Name of Item	Description	Compliance & Bidder Response (Y/N)
25	Use Case	Both BACH and Nikash as well as IDTP & RTGS applications should be supported to operate using the same HSM with same make and model without the need to procure any additional devices for these use cases.	
26	Key Replication	HSM should support automatic key replication between the HSMs part of the same High Availability group	
27	Migration	The vendor should configure the HSM to be operatable with Bangladesh Bank system (BACH-II, Nikash etc.) and guarantee post configuration backup are taken.	
28	Active Customer Base	Bidder must provide at least 5 references where the OEM's product is currently being used in Production	
29	Trained Resources	Bidder should have trained and certified resources locally in Bangladesh. Certified resources must have hands on experience of implementing HSM for BACH, Nikash system. Certificates of resources and UAT report at least from 2 Banks where bidder has implemented HSM for BACH and Nikash system need to be submitted.	