IPA/GAD/PCS 1X/HSM/2019 23/10/2019

To

Sub: Quote for Hardware Security Module (HSM)

Sir,

IPA intend to procure three Hardware Security Module (HSM) for keeping Digital Security Certificate , Keys to be used for used for file and payload encryption / decryption and digital signing.

We have requirement of Two HSM in HA in Data Centre(DC) which is in Mumbai and One HSM in Disaster Recovery(DR) which is in Bangalore.

Please submitted your quote as per below Bill of Materials (BOM) in the price bid (Annexure-I) at CCP portal

Sr. No.	***Product Description***	***Type***	***Validity***	***Qty***
1	Supply of Network HSM devices with OEM warranty	One-time	One-time for supply	3
2	Integration Support Charges	Per HSM	One-time	3
3	One Year Support Charge after warranty	ATS	Per Annum	3
4	Class 3 document signer certificate with 2 Yrs validity	Certificate	2 Yrs validity	3

Terms and Conditions:

- Payment Terms:50% Payment on Delivery and 50% Payment on Go live / Implementation
- Delivery: within 7 days from date of receipt of PO

The Network HSM Device should be in conformance to below mentioned specifications to meet the requirement of implementation in a cloud environment.

Security & Compliance:

- Keys shall always remain in FIPS-validated, tamper-evident hardware
- Meet compliance needs for GDPR, eIDAS, HIPAA, PCI-DSS etc.
- Should be De facto standard for the cloud
- Support multiple roles for strong separation of duties.
- Multi-person MofN with multi-factor authentication for increased security
- Support for secure audit logging
- High-assurance delivery with secure transport mode
- High quality keys through external Quantum RNG seeding

- Securely backup and duplicate keys in hardware for safekeeping in case of emergency, failure or disaster using SafeNet Luna Backup HSM

General Specifications:

- Support remote management of HSMs.
- Support for automation of enterprise systems to manage HSMs via REST API
- Ability to efficiently administer resources by sharing HSMs amongst multiple applications or tenants
- Support to flexible partition policies to meet out key management and compliance needs
- Support increased portability, greater efficiency and less overheads for using client in a container
- Support for Functionalities like
    - Extending native HSM functionality.
    - Develop and deploy custom code within the secure confines of the HSM

Security Certifications:

- FIPS 140-2 Level 3 – Password and Multi-Factor (PED)

Host Interface:

- Min. 4 Gigabit ethernet ports with port bonding
- Optional 10G fiber network connectivity with port bonding
- IPv4 and IPv6

Physical Characteristics:

- Standard 1U 19in. rack mountable appliance
- Input Voltage: 100-240V, 50-60Hz
- Power Consumption: 110W maximum, 84W typical
- Heat Dissipation: 376 BTU/hr maximum, 287 BTU/hr typical
- Temperature: operating 0°C – 35°C, storage -20°C – 60°C
- Relative Humidity: 5% to 95% (38°C) non-condensing

Reliability:

- Dual hot-swap power supplies
- Field-serviceable components
- Mean Time Between Failure (MTBF) 171,308 hrs

Management & Monitoring:

- Support for HA disaster recovery
- Ability for Backup and restore
- Support for SNMP, Syslog

Technical Specifications

- **Memory Support :** Min 2 MB
- **Partitions :** Min 1 , Max 5 partitions

Standard Performance:

Device must meet below mentioned minimum performance criteria basis various algorithms.

- For RSA-2048 algorithm : 1,000 tps
- For ECC P256 algorithm : 2,000 tps
- For AES-GCM algorithm : 2,000 tps

Operating environment support

- Operating Systems : Windows, Linux, Solaris, AIX
- Virtualization : VMware, Hyper-V, Xen, KVM

API Support

- PKCS#11, Java (JCA/JCE), Microsoft CAPI and CNG, OpenSSL
- REST API for administration

Cryptography

- Full Suite B support
- Asymmetric: RSA, DSA, Diffie-Hellman, Elliptic Curve Cryptography (ECDSA, ECDH, Ed25519, ECIES) with named, user-defined and Brainpool curves, KCDSA etc.
- Symmetric: AES, AES-GCM, Triple DES, DES, ARIA, SEED, RC2, RC4, RC5, CAST etc.
- Hash/Message Digest/HMAC: SHA-1, SHA-2, SM3 etc.
- Key Derivation: SP800-108 Counter Mode
- Key Wrapping: SP800-38F
- Random Number Generation: designed to comply with AIS 20/31 to DRG.4 using HW based true noise source alongside NIST 800-90A compliant CTR-DRBG
- Digital Wallet Encryption: BIP32

Quotes shall be addresses to :

Chief Administrative Officer
INDIAN PORTS ASSOCIATION
1ST FLOOR, SOUTH TOWER, NBCC PLACE,
BHISHAM PITAMAH MARG, LODI ROAD,
NEW DELHI 110 003
FAX 011-24365866
EPABX 24369061, 24369063 & 24368334
E mail: cao.ipa@nic.in

Please submit your Quote alongwith aforesaid technical details compliance at CPP portal by 30/10/2019 at 1530 Hrs.

s/d
(Rajeev Puri)
Chief Administrative Officer

Annexure-I

Price Bid

Sr. No.	***Product Description***	***Type***	***Validity***	***Qty***	***Price***	***GST***	***Total Price (incl GST)***
1	Supply of Network HSM devices with OEM warranty	One-time	One-time for supply	3			
2	Integration Support Charges	Per HSM	One-time	3			
3	One Year Support Charge after warranty	ATS	Per Annum	3			
4	Class 3 document signer certificate with 2 Yrs validity	Certificate	2 Yrs validity	3			