IPA/GAD/PCS 1X/HSM/2019 30/10/2019

Addendum no 1

[Quote for Hardware Security Module (HSM)]

1. Schedule for receipt of the Bid shall be read as follows:

    a. Submission of Bid on or before at 1530 Hrs on 01/11/2019.

    b. Opening of Bid at 1600 Hrs on 01/11/2019.

The Terms and condition shall be read as

Terms and Conditions:

- Payment Terms:50% Payment on Delivery and 50% Payment on Go live / Implementation
- Delivery: within 12 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:

- All Keys shall always remain in FIPS-validated, tamper-evident hardware
- Meet necessary compliance requirements for general purpose HSM to be used for digital Signing as well as encryption.
- Should be De facto standard for the cloud - (HSM should be compatible for fitment in a cloud environment)
- Support multiple roles for strong separation of duties.
- 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 dedicated Backup HSM

General Specifications:

- Support remote management of HSMs.
- Support for automation of enterprise systems to manage HSMs
- 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

Host Interface:

- Min. 4 Gigabit ethernet ports 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) 130,000 hrs(min)

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

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.

- 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

*****