F.No. HQ-25011/1/2022-IS-HQ
Government of India
Unique Identification Authority of India
(Information Security Division)

7th Floor, Bangla Sahib Road,
Gole Market, New Delhi-110001
Date: 18 August 2022

CIRCULAR

Subject: Detailed Technical Requirements for hardware based secure key management / exchange solution.

This is with reference to UIDAI Circular dated 15th June 2022 for POC environment setup to evaluate the Indian OEM's product/services to foster "Make in India" initiative in line with GOI guidelines.

2. UIDAI intends to offer PoC environment for hardware based secure key management / exchange solution to Indian OEMs or OEMs with 60% Indian content (as per MeitY guidelines for Cyber Security Products) in offered solution directly or through their authorized dealer. Broad specifications for the solution are as follows:

Sl.No	Technical Specifications
1	The hardware based secure key management / exchange solution should be a network based general purpose hardware security module with support of dual 10G NICs for fiber network connectivity
2	Device should support different VLANs for Production and Management
3	Support for minimum 9500 Transaction (Signing) per Second @ RSA 2048 bits
4	The proposed hardware based secure key management / exchange solution should be capable of expanding partitions upto 100 on same secure key management / exchange solution as business requirement grows in future.
5	The proposed hardware based secure key management / exchange solution should support dedicated management port and Rest APIs/Web based management console for restriction and automation of administrative traffic to specific servers.
6	The hardware based secure key management / exchange solution should have GUI capability for real time management and monitoring of secure key management / exchange solution including secure key management / exchange solution crypto resources, provisioning of secure key management / exchange solution partitions , dynamic secure key management / exchange solution status reports generation and up to date information on the status of secure key management / exchange solution device pool
7	Device shall be configured with HA mode

8	secure key management / exchange solution should be remotely manageable
9	Support for SNMP, Syslog
10	There should be no root or super-user access to hardware based secure key management / exchange solution appliance possible in any way. No access to bash , ksh or any default terminal shells should be possible.
11	OS-Support like Windows and all popular Linux flavours
12	Key Exchange Symmetric Algorithm: AES, ARIA, CAST, HMAC, SEED, Triple DES,
13	Support for PKCS#11, CAPI, OpenSSL, JCE/JCA and API for administration. **Should support secure web interface for administration and monitoring**
14	Support for Hash Message Digest HMAC, SHA1, SHA2 (512)
15	Support for various cryptographic algorithms: Asymmetric Key RSA (1024-4096 bits), DSA , (ECDSA, ECDH, Ed25519, ECIES)
16	Random Number Generation: should be designed to comply with AIS 20/31 to DRG.4 and also compliant to NIST 800-90A
17	Hardware based secure key management / exchange solution should support docker container based installation and usage without any 3rd party software use.
18	Hardware based secure key management / exchange solution should be scalable to support more signatures per second i.e. usable in cluster mode via secure key management / exchange solution library without the need for any external load balancer.
19	Should support Synchronization of keys between hardware based secure key management / exchange solutions on real-time basis as well as migration of existing keys in current production secure key management / exchange solution to newer secure key management / exchange solutions.
20	Should Support remote administration for maintaining partitions and adding or removing partitions as business required without the need for accessing hardware based secure key management / exchange solution physically in DC.
21	Hardware based secure key management / exchange solution Should have support for both Remote and Local multifactor authentication using PED Device & Keys for enhanced Security Support
22	Signed and tamper-evident event based audit logs and standard mechanisms for viewing logs should be available.
23	The solution and all the components there of must have provision for dual hot-swappable power supply.

3. All interested Indian OEMs may submit their brief proposal and specification as per UIDAI Circular dated 15/06/2022.

Sd/-

(Rashmirathi)
Deputy Director (IS)