

**CAIET DE SARCINI**  
**Bunuri/Servicii**

**Obiectul: Dispozitiv securizat de creare a semnăturii electronice de tip HSM**

**Autoritatea contractantă: I.P. Serviciul Tehnologia Informației și Securitate Cibernetică**

**Cryptography algorithms**

- Support for FIPS-approved and NIST recommended algorithms, modes, curves, and key sizes for RSA (up to 8192, sizes 2048, 3072 and 4096 are mandatory), DSA, Diffie-Hellman, AES, SHA-2 family, and Elliptic Curve Cryptography (ECC);
- NIST compliant Hardware Random Number Generator
- Asymmetric algorithms: RSA, DSA, Diffie-Hellman, Elliptic Curve Cryptography (ECDSA, ECDH, Ed25519, ECIES)
- Symmetric algorithms: AES, AES-GCM, DES, Triple DES, ARIA, SEED, RC2, RC4, RC5, CAST
- Hash/message digest: MD5, SHA-1, SHA-2 (224, 256, 384, 512 bit), HAS-160, RIPEMD160

**API Support**

- PKCS#11
- Microsoft CAPI and CNG
- Java (JCA or JCE)

**Performance**

- RSA-2048 signing ops > 8,000
- RSA-4096 signing ops > 3000
- ECC P256 signing ops > 8,000
- AES-GCM small packet encryption ops > 5,000

**Storage**

- Partitioning/virtual device/tenant support for logical delimitation of key pairs (> 50 partitions)
- Memory > 8MB

## **Supported Operating Systems**

- Windows Server: 2012R2, 2016, 2019
- Linux: RHEL / CentOS 6, 7, 8.

## **Security**

- Certified FIPS 140-2 minimum Level 3
- Multi-Tenancy support
- Remote Management

## **Network Interface**

- Minimum 2x Gigabit Ethernet ports
- IPv4 and IPv6

## **Physical Characteristics**

- Standard 1U/2U rack mount chassis
- Input Voltage: 100-240V, 50-60Hz
- Temperature: operating 0°C – 35°C, storage -20°C – 60°C
- Relative Humidity: 5% to 95% (38°C) noncondensing

## **Safety and Environmental Compliance**

- FCC, CE, UL, RoHS

## **Reliability**

- Dual hot-swap power supplies
- Field-serviceable components
- Mean Time Between Failure for security module(MTBF) over 300,000 hrs

## **Management and Monitoring**

- Remote configuration, administration, and monitoring
- High-Availability disaster recovery
- Backup and restore using FIPS 140-2 Level 2 Backup HSM
- Secure audit logging
- SNMP monitoring and diagnostics
- Syslog diagnostics support

## **Warranty policy and support**

- Minimum 2 years of warranty and tech support