

Product Brief

Luna PCIe HSM

cpl.thalesgroup.com

THALES
Building a future we can all trust

Secure sensitive data and critical applications by storing, protecting and managing cryptographic keys in Thales Luna PCIe HSMs – high-assurance, tamper-resistant PCIe cards. Provide applications with dedicated access to a purpose-built, high-performance cryptographic processor. Quickly embed this cost-efficient solution directly into servers and security appliances for FIPS 140-validated assurance.

Contact us to learn how Luna PCIe HSMs can help you ensure the integrity and protection of your encryption keys throughout their life cycle.

What you need to know:

Superior Performance & Usability

- Meet your high throughput requirements with over 20,000 ECC and 10,000 RSA operations per second for high performance use cases
- Lower latency for improved efficiency
- Dedicated access for applications
- Low profile PCIe card

Functionality Modules

- Extend native HSM functionality
- Develop and deploy custom code within the secure confines of the HSM

Highest Security & Compliance

- Keys always remain in FIPS-validated, tamper-evident hardware
- Meet regulation and compliance needs for GDPR, eIDAS, HIPAA, PCI-DSS, and more
- Multiple roles for strong separation of duties
- Multi-person MofN with multi-factor authentication for increased security
- Secure audit logging
- High-assurance delivery with secure transport mode

Technical specifications

Supported Operating Systems

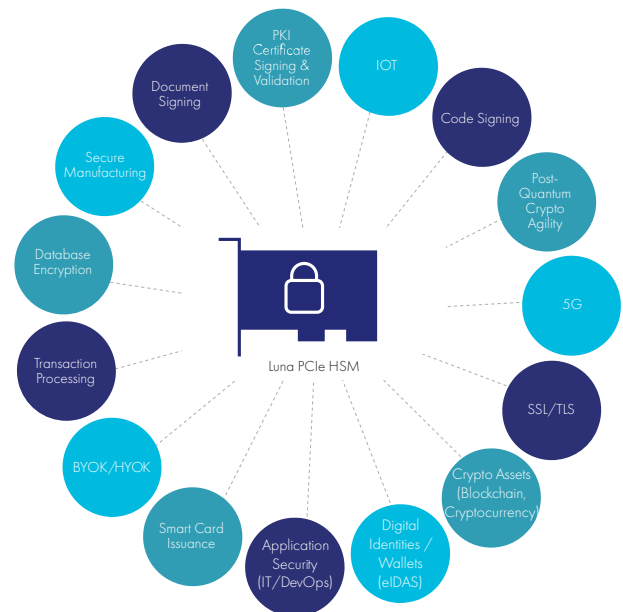
- Windows, Linux

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, and more
- Symmetric: AES, AES-GCM, Triple DES, DES, ARIA, SEED, RCS, RC4, RC5, CAST, and more



- 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
- Random Number Generation:
 - NIST SP 800-90 A/B/C certified
 - AIS 20/31 compliant to DRG.4
- Digital Wallet Encryption: BIP32

Security Certifications

- FIPS 140-2 Level 3 Validated – Password and Multi-Factor (PED)
- FIPS 140-3 Level 3 Validated – Password and Multi-Factor (PED)
- Common Criteria EAL4+ (AVA_VAN.5 and ALC_FLR.2) Certified against the Protection Profile EN 419 221-5
- Qualified Signature or Seal Creation Device (QSCD) listing for eIDAS compliance
- Singapore NITES Common Criteria Scheme
- Brazil INMETRO Approved (Formerly ITI)
- NATO Approved for Use up to Restricted

Physical Characteristics

- Low profile PCIe card
- Dimensions: 69.6mm x 167mm x 18.7mm (2.74" x 6.57" x 0.74")
- Power Consumption: 18W maximum, 14W typical

- Heat Dissipation: 61.4 BTU/hr maximum, 47.8 BTU/hr typical
- Temperature: operating 0°C–50°C, storage -20°C–60°C
- Relative Humidity: 5% to 95% (38°C) non-condensing

Safety & Environmental Compliance

- UL, CSA, CE
- FCC, CE, VCCI, C-TICK, KC MARK
- RoHS2, WEEE
- India BIS [IS 13252 (Part 1)/IEC 60950-1]

Host Interface

- PCI-Express CEM 3.0, PCI, PCI Express Base 2.0

Reliability

- Backup/restore
- High Availability (HA)
- Mean Time Between Failure (MTBF) 997,508 hours

Available models

Choose from two series of Luna PCIe HSMs, each one with 3 different models to fit your requirements.

Luna A Series:

Password Authentication for easy management.

Standard Performance A700	Enterprise Performance A750	Maximum Performance A790
Up to 4 MB Memory Performance: RSA-2048: 1,000 tps ECC P256: 2,000 tps AES-GCM: 2,000 tps	Up to 32 MB Memory Performance: RSA-2048: 5,000 tps ECC P256: 10,000 tps AES-GCM: 10,000 tps	Up to 64 MB Memory Performance: RSA-2048: 10,000 tps ECC P256: 22,000 tps AES-GCM: 17,000 tps

Luna S Series:

Multi-factor (PED) Authentication for high assurance use cases.

Standard Performance S700	Enterprise Performance S750	Maximum Performance S790
Up to 4 MB Memory Performance: RSA-2048: 1,000 tps ECC P256: 2,000 tps AES-GCM: 2,000 tps	Up to 32 MB Memory Performance: RSA-2048: 5,000 tps ECC P256: 10,000 tps AES-GCM: 10,000 tps	Up to 64 MB Memory Performance: RSA-2048: 10,000 tps ECC P256: 22,000 tps AES-GCM: 17,000 tps

tps = transactions per second