Product Brief

Luna PCIe HSM

Thales Trusted Cyber Technologies

thalestct.com

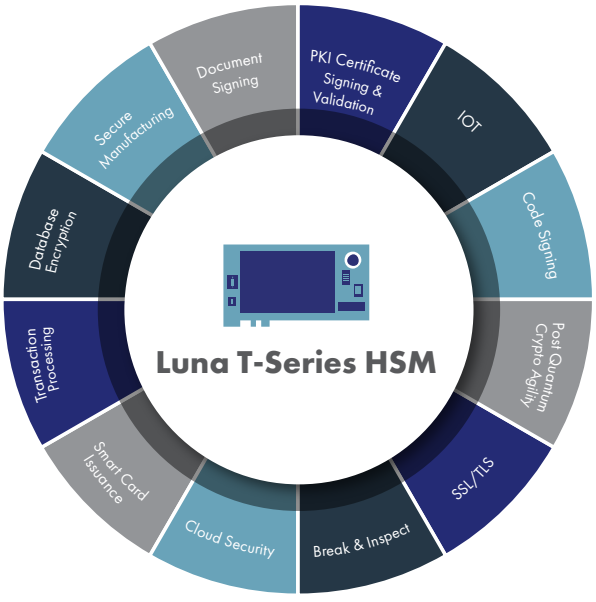
THALES
Building a future we can all trust

Luna PCIe Hardware Security Module (HSM) from Thales Trusted Cyber Technologies (TCT) is the choice for government agencies when generating, storing, protecting and managing cryptographic keys used to secure sensitive data and critical applications. Meeting government mandates for U.S. Supply Chain, the high assurance, tamper-resistant Luna T-Series HSM is designed, developed, manufactured, sold, and supported in the United States exclusively by Thales Trusted Cyber Technologies.

Luna T-Series models offer secure storage of your cryptographic information in a controlled and highly secure environment. All Luna T-Series models can be initialized by the customer to protect proprietary information by using either multifactor (PED) authentication or password authentication.

Industry Leading Performance & Security

- Industry leading cryptographic performance
- Performance optimized for government mandated algorithms and key lengths
- Up to 10 times the performance as compared to last-generation Luna PCIe for Government
- Keys-in-hardware approach protects the entire life-cycle of keys within the FIPS 140-2 validated confines of the HSM
- Addresses compliance requirements with FIPS 140 Level 3 certification
- Approved by CNSS for use in National Security Systems PKI



Crypto Agility

Thales TCT's Luna HSMs employ a crypto agile architecture that supports in-field introduction of new crypto algorithms. The Luna HSMs offer large amounts of memory (inside the crypto module) to support growth to larger key sizes. The Luna HSM's CPU capabilities support new, compute intensive algorithms and features.

Post-Quantum Cryptography (PQC) Algorithms

Thales TCT's Luna HSMs support ML-DSA and ML-KEM PQC algorithms as standardized by NIST. This enables agencies and technology partners to begin migrating their FIPS 140 Level 3 rooted cryptographic systems, guarding against Harvest Now, Decrypt Later and other quantum threats.

Additionally, the Luna HSMs support the Leighton-Micali Signature (LMS) stateful hash-based signature mechanism, along with its multi-tree variant, the Hierarchical Signature Scheme (HSS). Utilizing either LMS/HSS or ML-DSA, Luna HSMs enable customers to transition to quantumresistant firmware/software signing in accordance with CNSA 2.0.

Quantum Enhanced Keys

By embedding a quantum random number generator (QRNG) chip within the Luna HSM, Thales TCT is offering the industry's first FIPS 140-2 compliant HSM capable of generating quantum enhanced keys. Using principles of quantum physics, the QRNG chip produces high quality entropy which is the basis for all random numbers and cryptographic keys generated by the HSM. With a choice of operating the HSM in FIPS-approved mode using either the embedded, classic physical RNG or the embedded quantum RNG, customers can dynamically change between classical key generation and quantum enhanced keys as threats emerge over time.

Broad Integration Ecosystem

- Large number of integrations with industry-leading technology partners and vendors
- Documented, out-of-the-box integrations
- Video tutorials expedite integration tasks

Security First Company

- Trusted supplier to U.S. government for several decades
- HSM products are U.S. designed, developed and manufactured
- All employees are U.S. citizens
- All office locations in U.S.
- All support requests answered from U.S. (no outsourcing or foreign call centers)
- U.S. government approved Trusted Technology Import process
- Follow security best practices for all product introduction

Available Models and Performance

Luna PCIe HSM T-2000 Standard performance	**Luna PCIe HSM T-5000** Enterprise performance
16MB memory	32 MB memory
RSA 2048 1,400 tps	RSA 2048 14,000 tps
RSA 4096 350 tps	RSA 4096 3,500 tps
ECC P-256 3,000 tps	ECC P-256 16,000 tps
ECC P-384 2,000 tps	ECC P-384 16,000 tps

*tps is transactions per second

Technical Specifications

Cryptography

- Full support for NSA Commercial National Security Algorithm (CNSA) Suites 1.0 and 2.0
- Support for FIPS-approved and NIST recommended algorithms, modes, curves, and key sizes for RSA, DSA, Diffie-Hellman, AES, SHA-2, SHA-3 and Elliptic Curve Cryptography (ECC)
- Support for PQC algorithms: ML-DSA, ML-KEM, LMS/HSS
- NIST 800-90A compliant Hardware Random Number Generator
  - Classic hardware RNG entropy
  - Quantum RNG entropy
- Additional non-approved algorithms and key sizes are supported for use with legacy applications
- Refer to product documentation for complete details

API Support

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

Supported Operating Systems

- Windows Server: 2012R2, 2016, 2019, 2022
- Windows 10, 11
- Linux: RHEL / Rocky 8,9; Ubuntu 20, 22

Security Compliance

- FIPS 140-2 Level 3
- FIPS 140-3 Level 3*
- Approved by CNSS for use in National Security Systems PKI

Physical Characteristics

- Dimensions: Full Height, Half Length 4.2"x6.6"
- Weight: 300gm (10.6oz)
- Host Interface: PCIe Gen 2 x4
- Power Consumption: 20W maximum, 10W typical
- Temperature: operating 0°C – 50°C, storage -20°C – 60°C

Safety and Environmental Compliance

- FCC

Reliability

- Mean Time Between Failure (MTBF) 250,821 hrs
- HSM Battery Minimally Expected Lifetime: 10 Years

*in process

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., is a trusted, U.S. provider of cybersecurity solutions dedicated to U.S. Government. We protect the government's most vital data from the core to the cloud to the edge with a unified approach to data protection. Our solutions reduce the risks associated with the most critical attack vectors and address the government's most stringent encryption, key management, and access control requirements.

For more information, visit www.thalestct.com