

Thales Trusted Cyber Technologies Luna Hardware Security Modules



Hardware Security Modules (HSMs) are dedicated crypto processors designed to protect the cryptographic key lifecycle. HSMs serve as trust anchors that protect an organization's cryptographic infrastructure by securely managing, processing, and storing cryptographic keys inside a hardened, tamper resistant device.

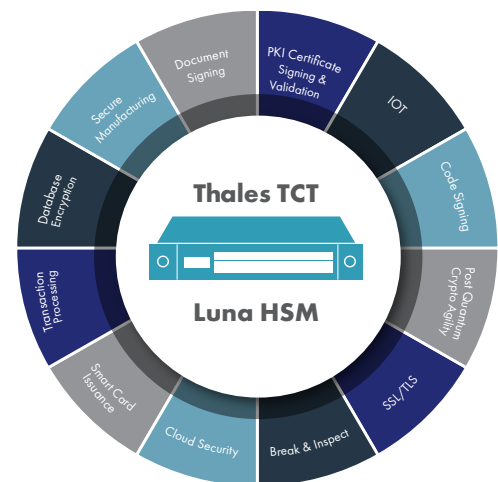
Thales Trusted Cyber Technologies' (TCT) Luna HSMs are the choice for government agencies when storing, protecting and managing cryptographic keys used to secure sensitive data and critical applications. Meeting government mandates for U.S. Supply Chain, the high-assurance, tamper-resistant Thales TCT's Luna HSMs are designed, developed, manufactured, sold, and supported in the United States.

Industry Leading Performance and Security

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

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.



Post-Quantum Cryptography (PQC) Algorithms

Thales TCT's Luna HSMs pre-standards implementations of NIST-selected PQC algorithms to facilitate agency and technology partner PQC testing. As a crypto agile product, Thales TCT will release software and firmware updates that comply with PQC standards once they are released.

Additionally, Thales TCT introduced the Leighton-Micali Signature (LMS) stateful hash-based signature mechanism, along with its multi-tree variant, the Hierarchical Signature Scheme (HSS). LMS/HSS enables customers to transition to quantum-resistant firmware/software signing in accordance with CNSA 2.0. Thales TCT's Luna HSM implementation of LMS is compliant with SP 800-208 and PKCS#11 v3.1.

Why Choose Thales TCT's Luna HSMs?

Security First Company

- U.S. Foundation (development, manufacturing, personnel, facilities)
- Strong security practices

Security and Compliance

- Address compliance requirements with FIPS 140 L3 and CNSS Approval
- Keys and certificates automatically generated and stored in hardware
- Maintain keys in hardware using the FIPS 140 L3 Luna Backup HSM

Scalability and High Availability

- Ability to have multiple applications share the same hardware
- Easy to add new applications – no new HSM required
- Ability to cluster HSMs to avoid single point of failure





Government Approval & Reference

- CNSS approval for TCT HSMs on National Security Systems
- NCCoE reference architecture for TLS Server Certificate Management
- Trusted supplier to U.S. Govt.

Partner Ecosystem

- Out-of-the-box integrations with third party applications
- Existing integrations that align with partner's future plans

Available Models

Luna Network HSM		Luna PCIe HSM		Luna G5	Luna as a Service	
						
Network-attached HSM that protects encryption keys used by applications in on-premise, virtual, and cloud environments		Embedded HSM that protects cryptographic keys and accelerates sensitive cryptographic operations		Compact, USB-attached HSM that is ideal for storing root cryptographic keys in an offline key storage device	Cloud-based HSM delivered through XTec's FedRAMP High authorized AuthenX Cloud	
Use Cases: PKI, SSL/TLS, Code Signing, Certificate Signing and Validation, Document Signing, Transaction Processing, DB Encryption, Smart Card Issuance		Use Case: Securing Custom Applications		Use Case: Offline Root CAs	Use Case: Cloud Smart Root-of-Trust, Anchoring applications across multiple cloud providers	
1U Appliance Dimensions: 19" x 21" x 1.725"		PCIe Card Dimensions: 4.2" x 6.6"		Mini Appliance Dimensions: 8.5" x 6.7" x 1.7"	No Hardware to Deploy	
Models		Models		Models	Models	
T-2000	T-5000	T-2000	T-5000	Luna G5	Dedicated HSM	Managed HSM
Standard Performance	Enterprise-level Performance	Standard Performance	Enterprise-level Performance	Use Case-Specific Performance	Enterprise-level Performance	Use Case Specific Performance
16MB memory	32 MB memory	16MB memory	32 MB memory	16 MB memory	32 MB memory	Up to 100 RSA 4096 Key Pairs
2 partitions, upgradable to 10	5 partitions, upgradable to 20	1 partition	1 partition	1 partition	5 or 20 partitions	1 Key Vault
RSA 2048 1,400 tps	RSA 2048 14,000 tps	RSA 2048 1,400 tps	RSA 2048 14,000 tps	RSA-2048 63 tps	RSA 2048 14,000 tps	RSA 2048 14,000 tps
RSA 4096 350 tps	RSA 4096 3,500 tps	RSA 4096 350 tps	RSA 4096 3,500 tps	RSA 4096 1 tps	RSA 4096 3,500 tps	RSA 4096 3,500 tps
ECC P-256 3,000 tps	ECC P-256 16,000 tps	ECC P-256 3,000 tps	ECC P-256 16,000 tps	ECC P256 4 3 tps	ECC P-256 16,000 tps	ECC P-256 16,000 tps
ECC P-384 2,000 tps	ECC P-384 16,000 tps	ECC P-384 2,000 tps	ECC P-384 16,000 tps	ECC P-384 6 tps	ECC P-384 16,000 tps	ECC P-384 16,000 tps

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