

Family Brief

Luna T-Series Hardware Security Modules

Quantum Ready,
U.S.-Built Security
for Mission Critical
Cryptographic Keys

thalestct.com

THALES
Building a future we can all trust

Hardware Security Modules (HSMs) are dedicated cryptographic processors that protect the full lifecycle of cryptographic keys. As hardened, tamper resistant roots-of-trust, they securely generate, manage, and store keys for sensitive data and mission critical applications.

Thales Trusted Cyber Technologies' (TCT) Luna T-Series HSMs are the trusted choice of U.S. government agencies, meeting U.S. supply chain requirements and delivering high assurance protection for modern PKI environments.

Post Quantum Cryptography

Luna T-Series HSMs are the first PQC-enabled HSMs manufactured in the U.S. to receive FIPS 140-3 Level 3 validation.

Luna T-Series HSMs support the government's transition to post quantum cryptography mandated by CNSA 2.0 and EO 14412. With support for ML-DSA, ML-KEM, and LMS/HSS, they safeguard long lived and mission critical data against emerging quantum threats.

Crypto Agility

Luna T-Series HSMs are crypto-agile and offer broad support for modern asymmetric and symmetric algorithms, hashing functions, and message authentication codes. A hardware based classical RNG and quantum RNG compliant with NIST SP 800-90A/B ensure high quality entropy for secure key generation.

Compliance Forged in the USA

Luna T-Series HSMs are FIPS 140-3 Inside (5450 & 5300), CNSS approved for National Security Systems PKI, and fully designed, manufactured, and supported in the United States. All Luna T-Series HSMs are built under a DCSA proxy and a CFIUS National Security Agreement to ensure trusted supply chain integrity.

Common Architecture

The entire Luna T-Series HSM portfolio—Network, PCIe, Mini, Tablet, and the FedRAMP High Authorized Luna as a Service—shares a unified architecture. With consistent clients, APIs, algorithms, and authentication methods, applications only need to be integrated once. Keys can be cloned securely across devices and across environments, from on premises deployments to the cloud.

Thales TCT's Luna T-Series HSMs— the First PQC-enabled HSMs Manufactured in the U.S. to Receive FIPS 140-3 Level 3 Validation.



FIPS 140-3 Inside (5450 & 5300)

Why Choose Thales TCT's Luna T-Series HSMs?

- Made in the USA for trusted federal supply chain compliance
- FIPS 140-3 Inside and CNSS approved for National Security Systems
- Post quantum ready with ML DSA, ML KEM, and LMS/HSS support
- Quantum enhanced key generation via embedded QRNG
- Broad crypto agility across modern algorithms
- Unified architecture for consistent APIs and easy key migration
- Flexible deployment from core to cloud to tactical edge
- Out-of-the-box integrations with third party applications
- Supports multiple apps on one HSM, scales easily, and clusters for high availability

HSMs for the Enterprise

	Luna Network HSM		Luna PCIe HSM		Luna as a Service	
						
Product Overview	Network attached HSM for on prem, virtual, and cloud environments		Embedded HSM for securing keys and accelerating cryptographic operations		Cloud based HSM delivered through XTec's FedRAMP High AuthenIX Cloud	
Use Cases	PKI, SSL/TLS, Code Signing, Certificate Signing & Validation, Document Signing, Transaction Processing, DB Encryption, Smart Card Issuance		Securing custom applications		Cloud Root of Trust; anchoring applications across multiple cloud providers	
Form Factors	1U Appliance Dimensions: 19" x 21" x 1.725"		PCIe Card Dimensions: 4.2 "x 6.6"		Cloud - No Hardware to Deploy	
Models	T-2000	T-5000	T-2000	T-5000	Dedicated HSM	Managed HSM
Memory	16 MB	32 MB	16 MB	32 MB	32 MB	Up to 100 RSA 4096 Key Pairs
Partition	2 up to 10	5 up to 20	1	1	5 or 20	1 Key Vault
RSA 2048	1,400	14,000	1,400	14,000	4,000	14,000
RSA 4096	350	3,500	350	3,500	3,500	3,500
ECC-P 256	3,000	16,000	3,000	16,000	16,000	16,000
ECC-P 384	2,000	16,000	2,000	16,000	16,000	16,000

HSMs for the Edge

	Tablet HSM	Mini HSM
		
Product Overview	Portable, USB HSM for offline storage of root keys	Small form factor HSM for tactical, remote, and edge deployments
Use Cases	Offline Root CAs	Secure mission critical keys in tactical, remote, and edge environments
Form Factors	Tablet	Mini Appliance
Models	T-300	T-400
Memory	32MB	32 MB
Partition	1	1
Dimensions	6.3" x 3.43" x 1.03"	7" x 5" x 1.5"
Weight	0.9lb (410g)	2.0lb (907kg)
Power Consumption	Max: 7.2W Typical: 4.5W	Max: 17.2W Typical: 14.5W
MIL-STD-810H	Not tested	Temperature, vibration, shock, and humidity

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