Product Brief



Luna T-Series Mini HSM

Industry First PQC-Enabled, MIL-SPEC, Tactical HSM for the Edge

thalestct.com

THALES
Building a future we can all trust

THALES

The Luna T-Series Mini HSM is a small form factor hardware root of trust purpose built to secure mission critical cryptographic keys in tactical, remote, and edge environments. Tested to military environmental standards, it delivers post quantum cryptography at mission speed through Thales TCT's FIPS 140 3 validated and CNSS approved M7 cryptographic module.

The Luna T-Series Mini HSM meets U.S. supply chain requirements and provides strong protection for a wide range of applications—including PKI root keys.

Root of Trust Anywhere

This compact HSM can operate standalone for tactical missions or integrate seamlessly into high availability groups with other Luna T-Series HSMs. It supports synchronous and asynchronous key replication and recovery from the core to the cloud to the edge, ensuring resilient, distributed security wherever it's needed.

Post Quantum Cryptography

Thales TCT's Luna HSMs lead the way in supporting 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, the Luna T-Series Mini HSM protects long lived, mission critical data against emerging quantum threats.

Crypto Agility

The Luna T-Series Mini HSM delivers full crypto agility with broad support for modern asymmetric and symmetric algorithms, standard hashing functions, and message authentication codes (MACs). It includes a hardware based random number generator compliant with NIST SP 800-90A/B, ensuring high quality entropy for secure key generation.

Compliance Forged in the USA

The Luna T-Series Mini HSM is FIPS 140 3 Inside (#5300), CNSS approved for use in National Security Systems PKI, and fully made in the USA. All Luna T-Series HSMs are designed, developed, manufactured, and supported domestically under a DCSA proxy and CFIUS National Security Agreement, ensuring trusted supply chain integrity.

Common Architecture

All Luna T-Series HSMs share a unified architecture—including Network, PCIe, Mini, Tablet, and Luna as a Service HSMs. With consistent clients, APIs, algorithms, and authentication methods, organizations gain flexibility and interoperability. Applications need to be designed only once, and keys can be cloned across HSMs and across deployment environments, from on-premises to the cloud.



Highlights

- Compact, MIL-SPEC hardware root of trust for tactical and edge deployments
- Post quantum protection with FIPS 140-3 validated, CNSS approved crypto
- U.S. designed, manufactured, and supported for trusted supply chain integrity
- Standalone or high availability deployment with secure key replication
- Support for CNSA 2.0 and EO 14412 post-quantum cryptographic algorithms: ML-DSA, ML-KEM, and LMS
- Broad crypto agility with modern algorithms and NIST compliant RNG
- Unified Luna architecture for consistent APIs and seamless key migration

Benefits & Features

High Assurance Security

- Keys stay protected inside FIPS 140-3 validated, intrusion resistant hardware
- Remote management plus backup and restore for fast disaster recovery
- Password authentication or Quorum (M of N) multi-factor authentication for stronger access control and separation of duties

Sample Applications

- PKI key generation and protection for online/offline CA keys
- CNSA 2.0-compliant software and firmware code signing
- Certificate validation and signing
- Root of trust for edge computing devices
- Supports Bring Your Own Key (BYOK) use cases

Technical Specifications

Luna T-Series Mini HSM (T-400)

- 1 partition, 32MB

Operating System Support

- Windows, Linux Client
- Cryptographic API Support
- PKCS#11, Java (JCA/JCE), Microsoft CAPI and CNG, OpenSSL

Cryptography

- Full support for NSA Commercial National Security Algorithm (CNSA) Suite
- Support for CNSA 2.0 and EO 14412 post-quantum cryptographic algorithms: ML-DSA, ML-KEM, and LMS
- 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)
- NIST 800-90A/B compliant Hardware Random Number Generator
- Additional non-approved algorithms and key sizes are supported for use with legacy applications

Security Certification

- FIPS 140-3 Level 3

Physical Characteristics

- Dimensions: 5" (w) x 7" (d) x 1.5" (h) 7" x 5" x 1.5" (127mm x 177.8mm x 38.1mm)
- Weight: 2.0lb (0.9kg)
- Operating Temperature: 3°C – 50°C | Storage Temperature: -40°C – 70°C
- Power Consumption: 17.2W maximum, 14.5W typical
- Interface: USB-C 3.0 Data, RJ45 Ethernet
- Embeddable chassis with multiple mounting points and 1U rack-mount shelf (sold separately)
- MIL-STD-810H tested for storage and operating temperature, vibration, shock, and humidity

Safety and Environmental Compliance

- FCC, UL, CE
- MIL-STD-810H

Reliability

- Crypto Module MTBF: 560073 hrs@40C, Telcordia SR-332, Issue C

Trade Agreement Compliance

- TAA

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

©2026 SafeNet Assured Technologies, LLC 111-5-26