

Product Brief

Luna T-Series Tablet HSM

Handheld Appliance

thalestct.com

THALES
Building a future we can all trust

THALES

The Luna T-Series Tablet HSM is a small form factor HSM that is widely used by government agencies to protect data, applications, and digital identities in order to reduce risk and ensure regulatory compliance. It is well suited for a wide variety of applications, including the strong protection of PKI root keys. Meeting government mandates for U.S. Supply Chain Luna T-Series Tablet HSM is designed, developed, manufactured, sold, and supported in the United States by Thales Trusted Cyber Technologies (TCT).

Luna T-Series Tablet HSM Overview

The Luna T-Series Tablet HSM delivers high assurance key protection, maintaining all key materials encrypted within the confines of the tamper-resistant hardware. The small form factor and offline key storage capability set the product apart, making it ideal for protecting mission critical keys in a secure offline environment.

Common Architecture

Luna T-Series HSMs benefit from a common architecture across the entire product line including Luna Network, Luna PCIe, and Luna as a Service HSMs where the client, APIs, algorithms, and authentication methods are consistent. This eliminates the need to design applications around a specific HSM, and provides the flexibility to clone keys from HSM to HSM and from on-premises to the cloud as your needs change.

Commercial National Security Algorithm (CNSA) Suite 2.0

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 140-3 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 quantum-resistant firmware/software signing in accordance with CNSA 2.0.

Crypto Agility

Luna T-Series Tablet HSM supports a broad range of asymmetric key encryption and key exchange capabilities, as well as support for all standard symmetric encryption algorithms. It also supports all standard hashing algorithms and message authentication codes (MAC). The Luna T-Series Tablet HSM has a hardware based random number generator, compliant with NIST SP 800-90A and B.



Highlights

- Portable, handheld, small form factor device
- Easy setup – up and running in minutes
- LCD display enables quick review of status including firmware, memory capacity, and more
- Host-powered USB – no need for an external power adaptor
- Support of Quorum (MofN) multi-factor authentication for increased security

Benefits & Features

High Assurance Security

- Keys always remain in FIPS 140-3 Level 3 validated, intrusion-resistant hardware
- Remote management, backup and restore for quick disaster recovery
- Password Authentication or Quorum (MofN) multi-factor authentication for increased security and strong separation of duties

Sample Applications

- PKI key generation and key storage/protection
- CNSA 2.0 compliant software and firmware code-signing
- Certificate validation and signing
- Offline hardware protection/security of critical keys
- Support Bring Your Own Key (BYOK) use cases

Performance Operation

Operation	Key	TPS
Sign	RSA-2048	62
Sign	RSA-4096	8
Sign	ECC P256	383
Sign	ML-DSA-87	20

*tps is transactions per second

Technical Specifications

Luna T-Series Tablet HSM (T-300)

- 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) 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 800-900A compliant Hardware Random Number Generator
- Additional non-approved algorithms and key sizes are supported for use with legacy applications
- Refer to product documentation for complete details

Security Certification

- FIPS 140-3 Level 3

Physical Characteristics

- Dimensions: 3.43" (w) x 1.03" (d) x 6.3" (h) (87.12mm x 160.02mm x 26.16mm)
- Weight: 0.9lb (410g)
- 4.7" LCD display
- Temperature:
  - Operating 0°C – 40°C
  - Storage -20°C – 70°C
- Relative Humidity: 20% to 95% (38°C) non-condensing
- Power Consumption: 7.2W maximum, 4.5W typical
- External USB AC: Input Voltage: 100 - 240V, 50 - 60Hz /Output 5VDC 3A
- Host Interface: USB 3.0 Type C connector
- Peripheral Interface: USB 3.0 Type C connector + USB-C (M) to USB-A (F) adapter

Safety and Environmental Compliance

- UL, CSA, CE
- FCC, KC Mark, VCCI, CE
- RoHS, WEEE

Reliability

- 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

©2024 SafeNet Assured Technologies, LLC 11-5-26