

Luna 8 Network HSM

The Foundation
of Digital Trust



Introducing the Luna 8 Network HSM

Quantum-Safe Root of Trust Delivering Scalable, Multi-Tenant, High-Performance Security and Reliability

Secure your sensitive data, identities and critical applications with Luna Network Hardware Security Modules (HSMs). Designed to securely store, protect, and manage cryptographic keys, these high-assurance, quantum-safe, tamper-resistant appliances deliver scalable, multi-tenant security and market-leading performance for post-quantum cryptography (PQC) workloads. Powered by the Thales custom-designed cryptographic processor, Luna 8 delivers high throughput, strong security isolation, and the crypto agility needed to quickly adapt to evolving business requirements, emerging threats, and new cryptographic algorithms.

Contact us to learn how our Luna Network HSMs can help you accelerate integration, secure the entire cryptographic key lifecycle in hardware, and simplify compliance. With support for a broad range of applications, Luna Network HSMs enable you to establish a quantum-safe root of trust that protects and future-proofs your entire cryptographic infrastructure.

Highest Security & Compliance

- Keys always remain in tamper-evident hardware
- Designed to meet compliance needs for GDPR, eIDAS, HIPAA, PCI-DSS, and more
- Multiple roles for strong separation of duties
- Quorum authorization with MofN and multi-factor authentication for increased security
- Side-channel protection for the Thales designed crypto processor
- High-assurance delivery with device attestation
- On-board dual entropy source (including QRNG) and support for external entropy source
- Securely backup keys in hardware with Luna Backup HSM for redundancy, reliability and disaster recovery

Scale and Optimize Operational Cost

- Each Thales HSM can contain one or two crypto modules; each crypto module is independent providing double the density for the same rack space
- Each crypto module can host up to 15x HSM instances, allowing a max of 30x HSM instances per appliance when configured with two crypto modules
- Run multiple Luna 8 firmware versions within secure containers on the same hardware
- Automate HSM administration and operational processes through APIs and CLI tools
- Integrate with existing IT infrastructure tools for monitoring, logging and metrics
- Out of band diagnostics and hardware utilization metricsFlexible security policies to meet your key management and compliance needs
- Increased portability, greater efficiency and less overhead using Luna Client in a container



Environmental by Design

Thales HSM demonstrate a measurable and significant decrease in our carbon footprint through eco-design. In alignment with Thales' ESG (environmental, social, and governance) commitment, Luna 8 is 20 x times more energy efficient per transaction compared to Luna 7.

Technical specifications

Supported Operating Systems

- Windows, Linux
- Virtual: VMware, Hyper-V, Xen, KVM

API Support

- PKCS#11, Java (JCA/JCE), Microsoft CAPI and CNG, OpenSSL
- APIs for administration

Post-Quantum Cryptography (PQC)

- ML-KEM (FIPS 203 key encapsulation) and ML-DSA (FIPS 204 digital signatures)
- Stateful Hash-Based Signatures: LMS and multi-level HSS (RFC 8554 / NIST SP 800-208)

Elliptic Curve Cryptography (ECC)

- Approved FIPS NIST Prime curves (P-192, P-224, P-256, P-384, P-521) and Brainpool curves (P192 through P512) for ECDSA/ECDH and ECIES
- Koblitz curve (secp256k1) for BIP32 Hierarchical Deterministic wallet key management
- Montgomery (X25519, X448) and Edwards (Ed25519, Ed448) curves

Asymmetric & Symmetric

- Asymmetric: RSA (up to 4096-bit key sizes) with standard PKCS#1 v1.5, OAEP, and FIPS-approved PSS probabilistic signature generation
- Symmetric: AES (128, 192, 256-bit) supporting ECB, CBC, CBC-PAD, CTR, GCM, GMAC, Key Wrap, and 512-bit AES-XTS mode. ARIA, SEED
- Legacy: Triple-DES (3DES) CBC/ECB preserved strictly for backwards-compatible unwrapping/decryption

Secure Hash, KDFs, and Telecom

- SHA-2 and SHA-3 secure hashing (224 to 512-bit) and HMAC
- SHAKE-128, SHAKE-256 Extendable-Output Functions (XOF)
- Key Derivation: NIST SP 800-108 Counter Mode
- Key Wrapping: NIST SP 800-38F
- 3GPP Mobile Telecom cellular security: MILENAGE, TUAK, and COMP128 subscriber authentication profiles

Digital Wallet & Blockchain Custody

- BIP32 and SLIP10 Hierarchical Deterministic (HD) Key Management

Random Number Generation

- Designed to comply with AIS 20/31 to DRG.4 using HW based true noise source alongside NIST 800-90A compliant HMAC_DRBG

Security Certifications

- FIPS 140-3 Level 3*
- Common Criteria EAL4+ (AVA_VAN.5 and ALC_FLR.2) Certified against the Protection Profile EN 419 221-5*
- Qualified Signature or Seal Creation Device (QSCD) listing for eIDAS 2 compliance*

Network

- 4x 10G SFP+ with multimode or single mode optical fiber and RJ45 copper
- IPv4, IPv6*, Port Bonding*
- 1 x 1G RJ45 ethernet port for Baseboard Management Controller (BMC)

Physical Characteristics

- Standard 1U 19in. rack mount appliance
- Dimensions:
 - 17.44" (W) x 21.95" (D) x 1.71" (H)
 - 443mm (W) x 557.6mm (D) x 43.5mm (H)
- Weight:
 - Single module appliance 26.5lbs (12kg)
 - Dual module appliance 30lbs (13.6Kg)
- Input Voltage: 100-240v AC, 50-60Hz
- Typical Power Consumption:
 - Single Module Appliance ~ 135W
 - Dual Module Appliance ~ 270W
- Max Power Consumption:
 - Single Module Appliance ~ 225W
 - Dual Module Appliance ~ 450W
- Temperature: operating 0°C – 40°C, storage -20°C – 60°C
- Relative Humidity: 5% to 95% (38°C) non-condensing

Safety & Environmental Compliance

- 80 PLUS Platinum Certified
- UL, CSA, CE
- FCC, CE
- RoHS3, WEEE
- TAA
- India BIS [IS 13252 (Part 1)/IEC 60950-1]*

Reliability

- Dual hot-swap power supplies and fans
- Mean Time Between Failure (MTBF)
 - Single Module Appliance: 289,444
 - Dual Module Appliance: 171,236

Management & Monitoring

- Quantum-safe HA failover / load balancing
- Quantum-safe backup and restore hardware to hardware
- rsyslog & BMC for out of band diagnostics



Available Luna Network HSM Models

MODELS			
	Luna 100 (Standard Performance)	Luna 150 (Enterprise Performance)	Luna 190 (Maximum Performance)
No. of Containers	1	Up to 6	Up to 15
Key Storage	128 MB	1024 MB	4096 MB

The Luna 8 Network HSM is available in three models based on performance, key capacity, and supported containers. Each model is tailored to common deployment requirements, making it easy to select the right solution for your environment. Each secure container hosts an isolated Luna 8 HSM instance and supports up to 10 partitions.

About Thales

Thales is a global leader in cybersecurity, helping businesses, governments, and the most trusted organizations in the world protect critical applications, sensitive data, identities, and software anywhere, at scale — with the highest ROI. With more than 30,000 customers, including 58% of the Fortune Global 500, our solutions are deployed in 148 countries around the world. Through our innovative services and integrated platforms, Thales helps customers achieve better visibility of risks, defend against cyber threats, close compliance gaps, and deliver trusted digital experiences for billions of consumers every day.