Product Brief

THALES

CYBERSECURITY

Luna Network HSM

cpl.thalesgroup.com

THALES

CYBERSECURITY

Secure your sensitive data and critical applications by storing, protecting and managing your cryptographic keys in Thales Luna Network Hardware Security Modules (HSMs) - high-assurance, tamper-resistant, network-attached appliances offering market-leading performance and crypto agility.

Contact us to learn how you can integrate Luna Network HSMs into a wide range of applications to accelerate cryptographic operations, secure the crypto key lifecycle, and provide a root of trust for your entire encryption infrastructure.

What you need to know:

Superior Performance:

- Meet your high throughput requirements with over 20,000 ECC and 10,000 RSA operations per second for high performance use cases
- Lower latency for improved efficiency

Highest Security & Compliance:

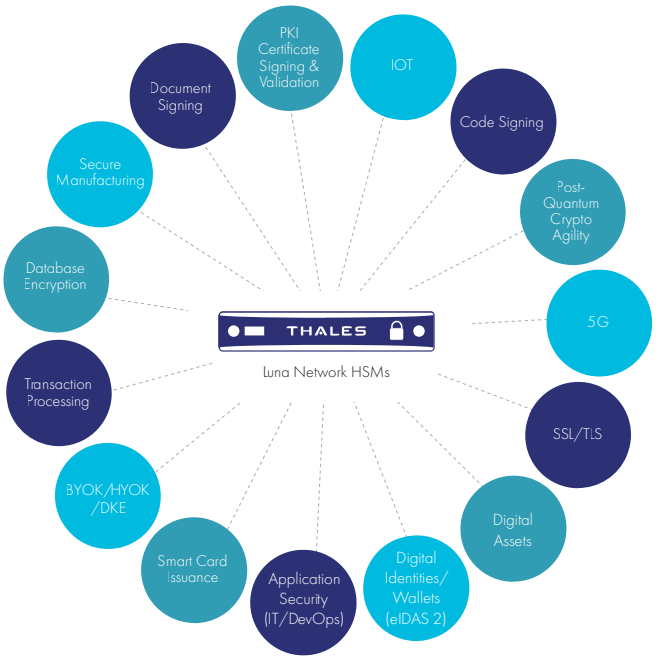
- Keys always remain in FIPS-validated, tamper-evident hardware
- Meet compliance needs for GDPR, eIDAS, HIPAA, PCI-DSS, and more
- De facto standard for the cloud
- Multiple roles for strong separation of duties
- Multi-person MofN with multi-factor authentication for increased security
- Secure audit logging
- High-assurance delivery with secure transport mode
- Strong keys with support for Dual (Internal / External) Entropy Sources and integrations with key QRNG vendors
- Securely backup and duplicate keys in hardware with Luna Backup HSM or to the cloud with Data Protection on Demand for redundancy, reliability and disaster recovery

Reduce Costs & Save time:

- Remotely manage HSMs - no need to travel
- Reduced audit and compliance costs and burdens
- Automate enterprise systems to manage HSMs via REST API
- Efficiently administer resources by sharing HSMs amongst multiple applications or tenants
- Flexible partition policies to meet your key management and compliance needs
- Increased portability, greater efficiency and less overhead using Luna Client in a container
- Functionality Modules
  - Extend native HSM functionality
  - Develop and deploy custom code within the secure confines of the HSM

Environmental by Design:

Thales Luna HSMs are dedicated to demonstrating a measurable and significant decrease in our carbon footprint, reducing power consumption and operating cost over each generation of HSM through eco-design, in alignment with Thales' ESG (environmental, social, and governance) commitment to a greener, safer world.



Technical specifications

Supported Operating Systems

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

API Support

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

Cryptography

- PQC Algorithms: ML-KEM (FIPS 203), ML-DSA (FIPS 204), SLH-DSA (FIPS 205)
- Full Suite B support
- Asymmetric: RSA, DSA, Diffie-Hellman, Elliptic Curve Cryptography (ECDSA, ECDH, Ed25519, ECIES) with named, user-defined and Brainpool curves, KCDSA, and more
- Symmetric: AES, AES-GCM, Triple DES, DES, ARIA, SEED, RC2, RC4, RC5, CAST, and more
- Hash/Message Digest/HMAC: SHA-1, SHA-2, SHA-3, SM2, SM3, SM4 and more
- Key Derivation: SP800-108 Counter Mode
- Key Wrapping: SP800-38F
- Random Number Generation: designed to comply with AIS 20/31 to DRG.4 using HW based true noise source alongside NIST 800-90A compliant CTR-DRBG
- Digital Wallet Key Management: BIP32 / SLIP10

5G Cryptographic Mechanisms for :

- Subscriber Authentication: Milenage, Tuak, and COMP128
- Subscriber Privacy Protection: ECIES

Security Certifications

- FIPS 140-2 Level 3 Validated – Password and Multi-Factor (PED)
- FIPS 140-3 Level 3 Validated – Password and Multi-Factor (PED)
- 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
- Brazil INMETRO Approved (Formerly ITI)
- Singapore NITES Common Criteria Scheme
- NATO approved for NATO SECRET on NATO/NCIA product catalogue

Host Interface

- IPv4 and IPv6
- Port Bonding
- **2 options:**
  - 4 x 1G RJ45 ethernet ports (default on all appliances)
  - 2 x 10G SFP+ Multimode for fiber network connectivity and 2 x 1G (790 models only)

Physical Characteristics

- Standard 1U 19in. rack mount appliance
- Dimensions: 19" x 21" x 1.725" (482.6mm x 533.4mm x 43.815mm)
- Weight: 28lb (12.7kg)
- Input Voltage: 100-240v AC, 50-60Hz
- Power Consumption: 100W maximum, 84W typical
- Heat Dissipation: 376BTU/hr maximum, 287BTU/hr typical
- Temperature: operating 0°C – 35°C, storage -20°C – 60°C
- Relative Humidity: 5% to 95% (38°C) non-condensing

Safety & Environmental Compliance

- 80 PLUS Silver Certified
- UL, CSA, CE
- FCC, CE, VCCI, C-TICK, KC Mark
- RoHS2, WEEE
- TAA
- India BIS [IS 13252 (Part 1)/IEC 60950-1]

Reliability

- Dual hot-swap power supplies
- Field-serviceable components
- Mean Time Between Failure (MTBF) 171,308 hrs

Management & Monitoring

- Quantum-safe HA Failover / Load Balancing
- Quantum-safe Backup and restore hardware to hardware on-premises or in the cloud
- SNMP, Syslog

Available models

Choose from two series of Luna Network HSMs, each one with 3 different models to fit your requirements.

Luna A Series:

Password Authentication for easy management.

Standard Performance A700	Enterprise Performance A750	Maximum Performance A790
Up to 4 MB Memory	Up to 32 MB Memory	Up to 64 MB Memory
Partitions: 5	Partitions: 5	Partitions: 10
Maximum Partitions: 5	Maximum Partitions: 20	Maximum Partitions: 100
Performance: RSA-2048: 1,000 tps ECC P256: 2,000 tps AES-GCM: 2,000 tps	**Performance:** RSA-2048: 5,000 tps ECC P256: 10,000 tps AES-GCM: 10,000 tps	**Performance:** RSA-2048: 10,000 tps ECC P256: 22,000 tps AES-GCM: 17,000 tps

Luna S Series:

Multi-factor (PED) Authentication for high assurance use cases.

Standard Performance S700	Enterprise Performance S750	Maximum Performance S790
Up to 4 MB Memory	Up to 32 MB Memory	Up to 64 MB Memory
Partitions: 5	Partitions: 5	Partitions: 10
Maximum Partitions: 5	Maximum Partitions: 20	Maximum Partitions: 100
Performance: RSA-2048: 1,000 tps ECC P256: 2,000 tps AES-GCM: 2,000 tps	**Performance:** RSA-2048: 5,000 tps ECC P256: 10,000 tps AES-GCM: 10,000 tps	**Performance:** RSA-2048: 10,000 tps ECC P256: 22,000 tps AES-GCM: 17,000 tps

tps = transactions per second

About Thales

Thales is a global leader in cybersecurity, helping the most trusted organizations protect critical applications, data, identities, and software anywhere, at scale. Through Thales' integrated platforms, customers achieve better visibility of risks, defend against cyber threats, close compliance gaps, and deliver trusted digital experiences for billions of consumers every day.

cpl.thalesgroup.com

Contact us – For contact information, please visit cpl.thalesgroup.com/contact-us