

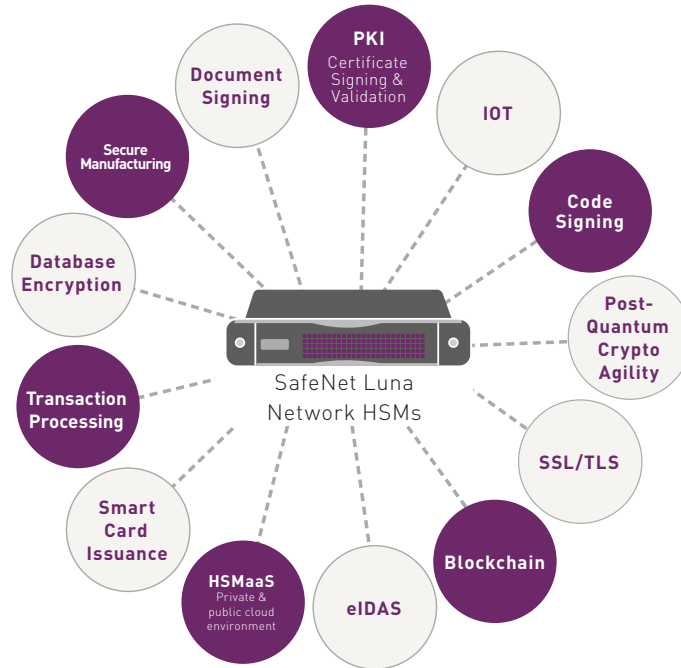


PRODUCT BRIEF

SafeNet Luna Network HSM

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

Contact us to learn how you can integrate SafeNet 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:

- > Fastest HSM on the market 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
- > High quality keys through external Quantum RNG seeding

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 SafeNet Luna Client in a container
- > Functionality Modules
 - > Extend native HSM functionality
 - > Develop and deploy custom code within the secure confines of the HSM

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

- > 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, SM3, 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 Encryption: BIP32

Security Certifications

- > FIPS 140-2 Level 3 – Password and Multi-Factor (PED)
- > eIDAS CC EAL4+ (AVA_VAN.5 and ALC_FLR.2) against the Protection Profile 419221-5 *

Host Interface

- > 4 Gigabit Ethernet ports with Port Bonding
- > IPv4 and IPv6

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, 50-60Hz
- > Power Consumption: 110W 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

- > UL, CSA, CE
- > FCC, CE, VCCI, C-TICK, KC Mark
- > RoHS2, WEEE
- > TAA

Reliability

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

Management & Monitoring

- > HA disaster recovery
- > Backup and restore
- > SNMP, Syslog

* under evaluation

Available Models

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

Luna A Series: Password Authentication for easy management.

A700	A750	A790
2 MB Memory	16 MB Memory	32 MB Memory
Partitions: 5	Partitions: 5	Partitions: 10
Maximum Partitions: 5	Maximum Partitions: 20	Maximum Partitions: 100
Standard Performance:	Enterprise Performance:	Maximum Performance:
> RSA-2048: 1,000 tps	> RSA-2048: 5,000 tps	> RSA-2048: 10,000 tps
> ECC P256: 2,000 tps	> ECC P256: 10,000 tps	> ECC P256: 22,000 tps
> AES-GCM: 2,000 tps	> AES-GCM: 10,000 tps	> AES-GCM: 17,000 tps

Luna S Series: Multi-factor (PED) Authentication for high assurance use cases.

S700	S750	S790
2 MB Memory	16 MB Memory	32 MB Memory
Partitions: 5	Partitions: 5	Partitions: 10
Maximum Partitions: 5	Maximum Partitions: 20	Maximum Partitions: 100
Standard Performance:	Enterprise Performance:	Maximum Performance:
> RSA-2048: 1,000 tps	> RSA-2048: 5,000 tps	> RSA-2048: 10,000 tps
> ECC P256: 2,000 tps	> ECC P256: 10,000 tps	> ECC P256: 22,000 tps
> AES-GCM: 2,000 tps	> AES-GCM: 10,000 tps	> AES-GCM: 17,000 tps

tsp = transactions per second

Contact Us: For all office locations and contact information, please visit safenet.gemalto.com/contact-us

Follow Us: blog.gemalto.com/security



THALES

gemalto
a Thales company