

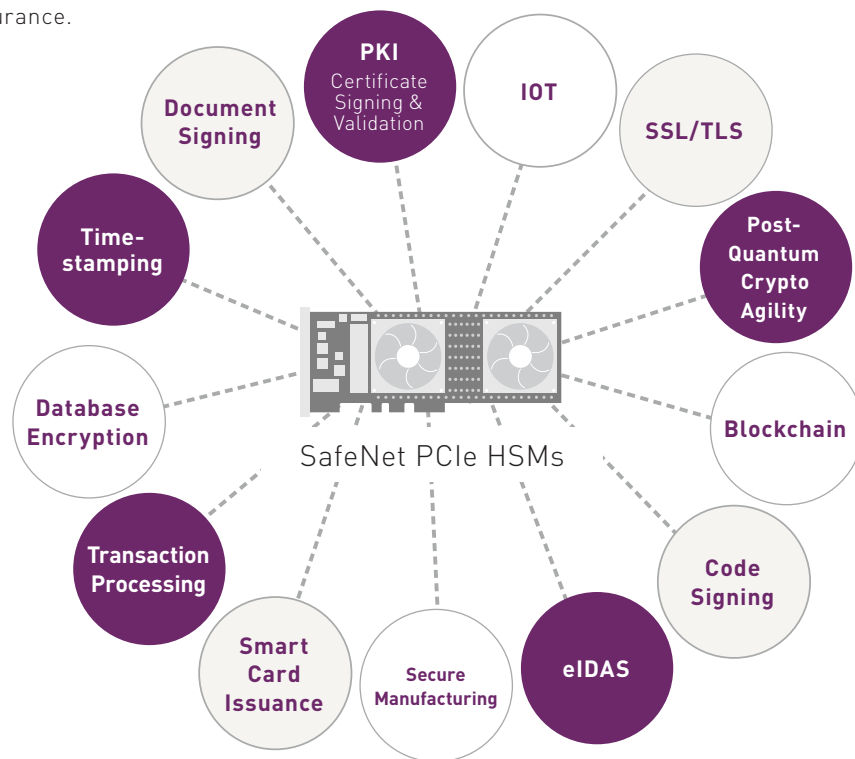


PRODUCT BRIEF

# SafeNet Luna PCIe HSM

Secure sensitive data and critical applications by storing, protecting and managing cryptographic keys in SafeNet Luna PCIe HSMs—high-assurance, tamper-resistant PCIe cards. Provide applications with dedicated access to a purpose-built, high-performance cryptographic processor. Quickly embed this cost-efficient solution directly into servers and security appliances for FIPS 140-2 validated assurance.

Contact us to learn how SafeNet Luna PCIe HSMs can help you ensure the integrity and protection of your encryption keys throughout their life cycle.



**What you need to know:**

**Superior Performance & Usability:**

- > 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
- > Dedicated access for applications
- > Low profile PCIe card

**Functionality Modules**

- > Extend native HSM functionality
- > Develop and deploy custom code within the secure confines of the HSM

**Highest Security & Compliance:**

- > Keys always remain in FIPS-validated, tamper-evident hardware
- > Meet compliance needs for GDPR, eIDAS, HIPAA, PCI-DSS, and more
- > 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

## Technical Specifications

### Supported Operating Systems

- > Windows, Linux

### API Support

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

### 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, RCS, 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 \*

### Physical Characteristics

- > Low profile PCIe card
- > Dimensions: 69.6mm x 167mm x 187mm (2.74" x 6.57" x 0.74")
- > Power Consumption: 18W maximum, 14W typical
- > Heat Dissipation: 61.4 BTU/hr maximum, 47.8 BTU/hr typical
- > Temperature: operating 0°C–50°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

### Host Interface

- > PCI-Express CEM 3.0, PCI, PCI Express Base 2.0

### Reliability:

- > Backup/restore
- > High Availability (HA)
- > Mean Time Between Failure (MTBF) 997,508 hours

\* under evaluation

## Available Models

Choose from two series of SafeNet Luna PCIe 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
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
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

tps = transactions per second

**Contact Us:** For all office locations and contact information, please visit [safenet.gemalto.com/contact-us](https://safenet.gemalto.com/contact-us)

**Follow Us:** [blog.gemalto.com/security](https://blog.gemalto.com/security)

 GEMALTO.COM

 **gemalto**  
security to be free