PRODUCT BRIEF

SafeNet Luna PCIe HSM

Versions 5.x and 6.x

> SafeNet Luna PCIe hardware security module (HSM) is the most secure cryptographic accelerator card in the industry. Designed for authentication, signing and key issuance, SafeNet Luna PCIe HSM is ideal for use as an embedded HSM in servers or appliances.

Secure Hardware Key Management

The high-assurance design of SafeNet Luna PCIe HSM offers dedicated hardware key management to protect sensitive cryptographic keys throughout the key lifecycle. The internal security architecture of SafeNet Luna PCIe HSM provides an unprecedented level of security for the keys and sensitive data generated, utilized, and stored within the HSM. At the core of SafeNet Luna PCIe HSM is the SafeXcel 3120, a robust, fail-safe security system on a chip used to protect internal keys and sensitive data. This defense-in-depth architecture isolates plaintext key material from the HSM's primary firmware by further encrypting internal keys with a key that exists only in the SafeXcel hardware.

Embed the SafeNet Luna General Purpose HSM Feature Set for Operational Cost Savings

SafeNet Luna PCIe HSM benefits from a robust and forward-thinking feature set. These features, including remote management, secure transport, and remote backup, will greatly reduce the management and operational costs of a solution.

High-Availability and Scalability

Multiple SafeNet Luna PCIe cards can be grouped together in the same server to provide high availability (HA), load balancing, and scalable performance. The HA group technology shares the transaction load, synchronizes data among members of the group, and redistributes the processing capacity in the event of failure in a member card to maintain uninterrupted service. The HA capability also enables easy recovery when a unit returns to service. SafeNet Luna PCIe HSM also includes API support for the synchronization of keys between cards in different servers. Using this API, organizations can create their own HA setup.

Benefits & Features

Most Secure

- Keys in hardware
- Remote management
- Secure transport mode for high-assurance delivery
- Multi-level access control
- Multi-part splits for all access control keys
- Intrusion-resistant, tamper-evident hardware
- Secure Audit Logging
- Strongest cryptographic algorithms
- Suite B algorithm support
- Secure decommission

Sample Applications

- PKI key generation and storage
- Storage (online and offline CA keys)
- Certificate validation and signing
- Document signing including remote signing use cases
- Transaction processing
- Database encryption
- Smart card issuance

Flexible Backup and Disaster Recovery Options

SafeNet Luna PCIe HSM provides secure, auditable and flexible options to simplify backup, duplication, and disaster recovery. Key backups can be performed locally or remotely to the SafeNet Luna Backup HSM.

Achieve FIPS 140-2 and Common Criteria Validation without Investing in Costly Certifications

Achieving FIPS or Common Criteria certification can be a time-consuming and costly process. As Gemalto's sole focus is security, we make third-party certifications a priority. Our team has years of experience in designing products that adhere to FIPS 140-2 and Common Criteria. Leveraging SafeNet Luna PCIe HSMs in your appliance or service represents a cost-effective way to bring FIPS and Common Criteria-validated solutions to market.

Develop Solutions for Resource Constrained Environments with ECC Support

As the need to provide security for resource-constrained devices (smart phones, tablets, smart meters) grows, vendors must be able to provide solutions that leverage ECC algorithms. ECC offers high key strength, at a greatly reduced key length when compared to RSA keys. SafeNet Luna PCIe HSM offers hardware-accelerated ECC algorithms that can be used in the development of solutions without the need to purchase additional licenses.

Common SafeNet Luna Domain

All SafeNet Luna HSMs benefit from a Common SafeNet Luna Architecture where the supported client, APIs, algorithms, and authentication methods are consistent across the entire SafeNet Luna HSM product line. This eliminates the need to design applications around a specific HSM, and provides the flexibility to move keys from form factor to form factor.

Available in Two Performance Models

- **SafeNet Luna PCIe HSM 7000** offers high performance across a breadth of algorithms including ECC, RSA, and symmetric transactions.
- **SafeNet Luna PCIe HSM 1700** is capable of 1700 RSA 1024-bit transactions per second (tps).

Technical Specifications

Operating System Support
- Windows, Linux, Solaris

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

Cryptography
- Full Suite B support
- Asymmetric: RSA (1024-8192), DSA (1024-3072), Diffie-Hellman, KCDSA, Elliptic Curve Cryptography (ECDSA, ECDH, ECIES) with named, user-defined and Brainpool curves
- Symmetric: AES, RC2, RC4, RC5, CAST, DES, Triple DES, ARIA, SEED
- Hash/Message Digest/HMAC: SHA-1, SHA-2 (224-512), SSL3-MD5-MAC, SSL3-SHA-1-MAC
- Random Number Generation:
  FIPS 140-2 approved DRBG
  (SP 800-90 CTR mode)

Physical Characteristics
- Dimensions: Full Height, Half Length 4.16" x 6.6" (106.7mm x 167.65mm)
- Power Consumption: 12W maximum, 8W typical
- Temperature: operating 0°C – 50°C

Security Certifications (SA, PCI-E, G5)
- FIPS 140-2 Level 2 and Level 3
- Common Criteria EAL 4+ (AVA_VAN.5)
- BAC & EAC ePassport Support
- NITES

Safety and Environmental Compliance
- UL, CSA, CE
- FCC, KC Mark, VCCI, CE
- RoHS, WEEE

Host Interface
- PCI-Express X4, PCI CEM 1.0a

Reliability
- MTBF 1,000,000 hrs

Algorithm	Model	
	SafeNet Luna PCIe 1700	SafeNet Luna PCIe 7000
RSA-1024	1,700 (tps)	7,000 (tps)
RSA-2048	360 (tps)	1,200 (tps)
ECC P256	580 (tps)	2,000 (tps)
ECIES	200 (tps)	310 (tps)
AES-GCM	3,600 (tps)	3,600 (tps)

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

Follow Us: blog.gemalto.com/security/

GEMALTO.COM

gemalto
security to be free

©Gemalto 2018. All rights reserved. Gemalto, the Gemalto logo, are trademarks and service marks of Gemalto and are registered in certain countries. PB (EN)-Jun.22.2018 - Design: ELC