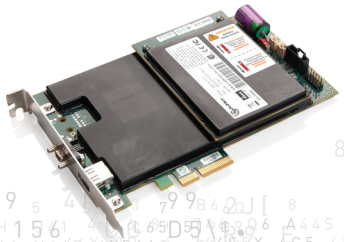
SafeNet | THE DATA PROTECTION COMPANY



Luna PCI-E:

Hardware Security Module (HSM)

PRODUCT BRIEF

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 & key
- Storage (online CA keys & offline CA keys)
- Certificate validation & signing
- Document signing
- Transaction processing
- Database encryption
- Smart card issuance

Luna PCI-E is the fastest and most secure cryptographic accelerator card in the industry and is widely used by major governments, financial institutions, and large enterprises for data, applications, and digital identities to reduce risk and ensure regulatory compliance.

Secure Hardware Key Management

Luna PCI-E improves upon the performance and security of the Luna PCI product family. For maximum security, the high assurance design of Luna PCI-E offers dedicated hardware key management to protect sensitive cryptographic keys throughout the key lifecycle, including key generation, storage, and backup.

Luna PCI-E can be embedded directly in an application server for an easy-to-integrate and cost-efficient solution for cryptographic acceleration. Luna PCI-E supports a broad range of asymmetric key encryption and key exchange capabilities, as well as support for all standard symmetric encryption algorithms. It also supports all standard hashing algorithms and message authentication codes (MAC). Enhancing the previous generation HSM's support of factory-generated digital IDs based on RSA key pairs, Luna PCI-E also supports ECC key pairs for use in Suite B applications that require a permanent, factory-generated digital ID. ECC algorithms are designed to use smaller key lengths to offer the same level of security as RSA-based algorithms. This allows devices with limited processing power to achieve a high level of security without sacrificing expensive computing cycles and with minimal effect on application performance.

Available in Two Performance Models

Luna PCI-E is available in two performance models; Luna PCI-E 7000 and Luna PCI-E 1700. Luna PCI-E 7000 is a high performance HSM capable of best in class performance across a breadth of algorithms including ECC, RSA, and symmetric transactions. The low performance variant, Luna PCI-E 1700, is capable of 1700 RSA 1024-bit transactions per second.

Algorithm	Model	
	Luna PCI-E 1700	Luna PCI-E 7000
RSA-1024	1,700	7,000
RSA-2048	350	1,200
ECC P256	500	1,000
ECIES	200	300
AES-GCM	3,700	3,900

High-Availability and Scalability

When used within the same server, Luna PCI-E fully manages key synchronization for high availability and load balancing, providing greater availability and scale in performance. Luna PCI-E also includes API support for synchronization of keys between cards in different servers. Using this API, organizations can create their own high-availability setup. The high availability features of Luna PCI-E also provide scalable performance. A high-availability group with three

Technical Specifications

Operating System Support
- Windows, Linux, Solaris

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

Cryptographic
- 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 EAL4+**
- BAC & EAC ePassport Support

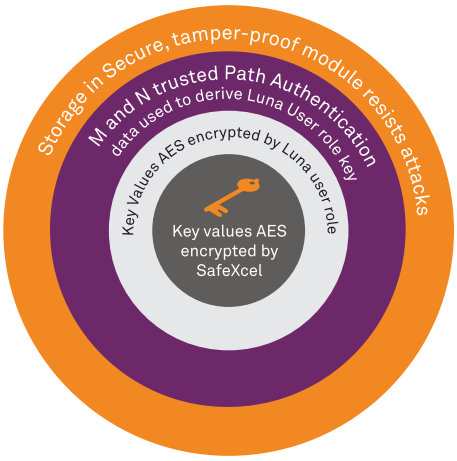
**Under evaluation

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 216, 204 hrs

Luna PCI-E 7000 cards, for example, is capable of performances up to 18,000 RSA 1024-bit signings per second and 3,600 RSA 2048-bit signings.



Fail-Safe Security Architecture

The internal security architecture of Luna PCI-E provides an unprecedented level of security for the keys and sensitive data generated, utilized, and stored within the HSM. At the core of Luna PCI-E 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. Utilization of split key techniques provides an enhanced tamper response feature triggered by the detection of external attack or an internal hardware anomaly.

The SafeXcel-3120 and SafeXcel-1746 perform all of the cryptographic operations for NIST-approved algorithms. Modeled after the high-assurance U.S. government chips that SafeNet develops today, the SafeXcel-3120 acts as a trust anchor, utilizing a secure boot process to ensure that only trusted firmware runs within the HSM. In addition to its previously described key management role, the SafeXcel-3120 performs all key generation for NIST-approved algorithms, and is used for signing, verification, encryption, and decryption in medium-performance environments. When used in a high performance environment, the HSM automatically offloads the cryptographic computations to the SafeXcel-1746, a sophisticated security co-processor chip.

All Luna HSMs are securely packaged inside specially designed enclosures to meet stringent requirements for tamper and intrusion resistance. The Luna PCI-E features sophisticated tamper detection and response circuitry that will automatically zeroize internal keys in the event of an attempted attack on the HSM. Balancing this extreme security posture with end user ease-of-use concerns, the Luna PCI-E includes a capability for properly authenticated security officers to recover from an inadvertent tamper event, and quickly put the HSM back into its usable state without the loss of any keys or sensitive data.

Cost-Saving Features

Luna PCI-E benefits from a diverse feature set that enables greater centralized control through secure remote management, transport, and backup. These features eliminate costs accrued from sending personnel to remote offices or data centers for HSM administration and management.

- **Luna Remote PIN Entry Device (PED)** is a multi-factor authentication console that uses a highly secure trusted channel between the PED and HSM across any network to allow for remote management and administration of the HSM.
- **Secure Transport Mode** enables Security Officers to use the device's tamper recovery role keys to cryptographically lock down the HSM prior to transporting the device. The recovery role keys can be shipped separately and re-combined at the destination to cryptographically verify the HSM's integrity.
- **Remote Backup HSM** enables the storage of objects from multiple PCI cards remotely and securely. With a single SafeNet Luna Backup HSM, an administrator can back up and restore keys to and from up to 20 Luna HSMs.

Contact Us: For all office locations and contact information, please visit **www.safenet-inc.com**
Follow Us: www.safenet-inc.com/connected