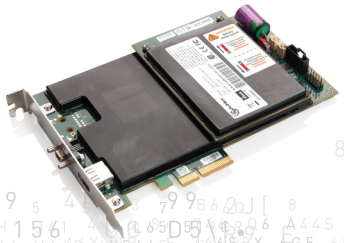
SafeNet | THE DATA PROTECTION COMPANY



Luna PCI-E 5.0 Hardware Security Module (HSM)

PRODUCT BRIEF

Benefits

- Keys remain in hardware for maximum security
- PCI-E form factor permits the development of OEM crypto solutions
- Ease of management for a lower total cost of ownership with remote management and backup features
- Secure and cost-effective deployment with secure transport mode
- Lower cost option where a network-attached appliance is not required

Features

- High-Assurance HSM design
- Fastest Cryptographic PCI Express Accelerator Card on the market
- Secure Authentication and Access Control
- PCI Express compatible
- Full Cryptographic API support
- Toolkits for easy integration
- Fail Safe Security Architecture
- Defense-in-depth internal key hierarchy
- Improved tamper detection and response
- Optimized for Suite B performance
- Factory-Installed ECC digital ID
- Remote PED
- Remote Backup HSM
- HA and Load Balancing within same server
- Secure Transport Mode

Luna PCI-E 5.0 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 5.0 improves upon the performance and security of the Luna PCI product family. For maximum security, the high assurance design of Luna PCI-E 5.0 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 5.0 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 5.0 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.

Like its predecessors, Luna PCI-E 5.0 continues to offer high-performance cryptographic processing at a rate of 7,000 1024-bit RSA operations per second and over 1,200 2048-bit RSA operations per second. The Luna PCI-E 5.0 also offers market-leading Suite B performance and can process up to 1,800 Elliptic Curve Digital Signature Algorithm (ECDSA) operations per second using the NIST P-256 ECC curve. The combination of RSA and ECDSA performance makes Luna PCI-E 5.0 the natural choice for security-conscious customers deploying the new generation of Suite B applications or for customers that just want to future-proof their deployments. Symmetric encryption capabilities have also been substantially improved with the Luna PCI-E 5.0, providing 500 Mbps of AES throughput.

When used within the same server, Luna PCI-E 5.0 fully manages key synchronization for high availability and load balancing, providing greater availability and scale in performance. Luna PCI-E 5.0 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 5.0 also provide scalable performance. A high-availability group with three Luna PCI-E cards, for example, is capable of performances up to 18,000 RSA 1024-bit signings per second and 3,600 RSA 2048-bit signings.

Technical Specifications

Client API Support
- PKCS#11 v2.20
- Microsoft CryptoAPI and CNG
- Java JCA/JCE
- OpenSSL

Operating System Support
- Windows 2003 (32 and 64-bit, Windows Server2008R2 (64-bit)
- Solaris 10 (32 & 64-bit)
- Linux E4, E5 K2.6 (32 & 64-bit)

Cryptographic Processing

Asymmetric Keys
- RSA (1024-4096 bit), PKCS #1v1.5,
- OAEP PKCS#1 v2.0
- Diffie-Hellman (DH) (1024 bit)
- Elliptic Curve Diffie-Hellman (ECDH) (numerous curves supported)

Digital Signing and Verification
- RSA (1024-8192-bit), DSA (1024-3072-bit), PKCS#1 v1.5, ECDSA (numerous curves supported), KCDSA

ECC Support
- ECDSA, ECDH
- Numerous curves supported, including NIST P-curves up to P-521, Brainpool Curves, and user-defined curves.

Symmetric Key Algorithms
- TDES (double & triple key lengths), RC4, RC5, AES, SEED, ARIA

Message Digest Algorithms
- SHA-1, MD-5, HAS-160, SHA224, SHA256, SHA384, SHA512

Message Authentication Codes
- HMAC-MD5, HMAC-SHA-1, HMACSHA-224, HMAC-SHA-256, HMACSHA- 384, HMAC-SHA-512, SSL3-MD5-MAC, SSL3-SHA-1-MAC

Complete NSA Suite B Algorithms
- AES-128, AES-256
- ECDSA P-256, P-384
- ECDH P-256, P-384
- SHA-256, SHA-384

Random Number Generation
- AES-DRBG per NIST 800-90

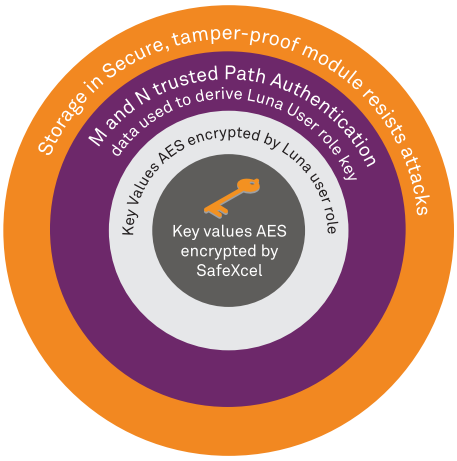
Certifications

Compliance
- FIPS 140-2 Level 2 and Level 3 validation (in process)
- BAC and EAC ePassport Support
- DIRECTIVE 2002/95/EC of the European
- Parliament and Council (ROHS)

Safety
- CSA C22.2 N0 950 NRTL/C
- EN 60950-1
- IEC 60950-1

Emissions
- EN 55022:1988 + amendment A1:2000
- + amendment A2:2003
- EN 55024 + amendment A1:2001 +
- amendment A2:2003
- FCC Part 15 Subpart B, Class B
- VCCI

Fail-Safe Security Architecture



The internal security architecture of Luna PCI-E 5.0 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 5.0 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 5.0 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 5.0 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