



Luna® PCI 7000 Hardware Security Module (HSM)

PRODUCT BRIEF

Benefits

- Fastest Cryptographic PCI Accelerator Card on the Market
- Secure Authentication and Access Control
- PCI express bus plugs into host computer
- Full Cryptographic API Support and Developer’s Toolkits for Easy Integration

Luna PCI 7000 is the fastest, most secure, cryptographic PCI accelerator card in the industry, and is widely used by major governments, financial institutions and large enterprises around the world. The PCI-X, and PCI express bus on Luna PCI 7000 easily plugs into the host computer and provides reliable protection for data, applications, and digital identities to reduce risk and ensure regulatory compliance.

Secure Hardware Key Management

For maximum security, Luna PCI 7000 offers dedicated hardware key management to protect sensitive cryptographic keys from attack. The high security design ensures the integrity and protection of encryption keys throughout their life cycle. Luna PCI HSMs provide hardware secure key generation, storage, secure key backup and accelerated encryption in a range of models and configurations, offering a wide selection of security, performance and operational capabilities. Luna PCI 7000 is securely packaged to meet the most stringent requirements for tamper and intrusion resistance.

High-Performance Cryptographic Processing

Luna PCI 7000 offers high-performance cryptographic processing at a rate of 7,000 asymmetric 1024-bit RSA operations per second—more than twice as fast as the nearest competitor—and it can be embedded directly in an application server for an easy-to-integrate and cost efficient security solution.

Secure Authentication and Access Control

To prevent unauthorized access to sensitive cryptographic material, Luna PCI 7000 offers strong two-factor authentication and multiple administrator roles. Luna PCI 7000 also offers true Trusted Path Authentication using the Luna PED (PIN Entry Device) which is an integrated handheld authentication console that does not rely on commercial keyboards or displays for administrator PIN code entry.

Certified Hardware
<ul style="list-style-type: none"> • FIPS 140-2 Level 2 and Level 3 validation • Common Criteria at EAL 4+ • RoHS compliant

Client API Support
<ul style="list-style-type: none"> • PKCS#11 v2.01 • Microsoft CryptoAPI 2.0 • Java JCA/JCE • Open SSL

Technical Specifications

Operating System Support

- Win 2003 (64-bit)
- Windows Server 2008 (64-bit)
- Solaris 9, 10 (32 & 64-bit)
- Linux E4, E5 2.6

Cryptographic Processing

Asymmetric Key Encryption and Key Exchange

- RSA (1024-4096 bit), PKCS #1 v1.5, OAEP PKCS#1 v2.0
- Diffie-Hellman (1024 bit)

Suite B Algorithm Support

ECC Support

- ECDSA
- ECC Brainpool Curves (named and user-defined)

Digital Signing

- RSA (1024-4096-bit), DSA (1024-bit), PKCS #1 v1.5

Symmetric Key Algorithms

- DES, 3DES (double & triple key lengths), RC2, RC4, RC5, CAST-3, CAST-128, AES

Message Digest Algorithms

- SHA-1, SHA-224, SHA-256, SHA-384, SHA-512

Message Authentication Codes

- HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512, SSL3-MD5-MAC, SSL3-SHA-1-MAC

Random Number Generation

- Luna PCI supports random number generation based on Appendix A 2.4 of ANSI X9.31
- 1280 Object Limit

Physical Characteristics

Card type

- PCI Card, Universal

Operating Temperature

- 0°C to 40°C

Storage Temperature

- -20°C to +65°C

Power Requirements

- +5V@3A Max; +12V@0.2A Max (FIPS Level 3 only)

Dimensions

- 4.1" by 7.88"

Connectivity

- PCI-X r1.0b

PCI Module

- Full Height 7.88" length
- PCI Module PCI-X r1.0b compliant at 64-bit 66MHz
- PCI 2.3 compatible at 33/66 MHz, 32/64-bit
- PCI Express Bus

Cryptographic Capabilities

Luna PCI 7000 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), as well as Random Number Generation based on Appendix A 2.4 of ANSI X9.31.

Enterprise Data Protection

SafeNet Luna PCI 7000 is a key component of SafeNet's comprehensive enterprise data protection solution to reduce the cost and complexity of regulatory compliance, data privacy, and information risk management. SafeNet Enterprise Data Protection (EDP) is the only solution that secures data across the connected enterprise, from core to edge, with protection of data at rest, data in transit, and data in use. Unlike disparate, multi-vendor point solutions that can create limited "islands" of security, SafeNet EDP provides an integrated security platform with centralized policy management and reporting for seamless, cost-efficient management of encrypted data across databases, applications, networks, and endpoint devices. For more information, visit www.safenet-inc.com/EDP



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

Follow Us: www.safenet-inc.com/connected

©2010 SafeNet, Inc. All rights reserved. SafeNet and SafeNet logo are registered trademarks of SafeNet. All other product names are trademarks of their respective owners. PB (EN)-08.19.10