

Luna® PCM 2.4 Key Management System is a dedicated Hardware Security Module (HSM) designed to provide the highest levels of performance and protection.



Benefits

Most Robust Hardware Backup and Physical Security

Suite B Algorithm Support

ECC Support

Easy to Integrate

Built for HSM Best Practices

FIPS 140-2 L 2 Validated

Secure Hardware Key Management

Luna PCM 2.4 features industry-leading hardware key management. All key materials used by Luna PCM 2.4 are maintained exclusively within the confines of Luna PCM 2.4's cryptographic hardware: from creation, to storage, to use, and destruction, sensitive cryptographic keys are never exposed outside of Luna PCM 2.4.

Hardware Cryptographic Processing

Luna PCM 2.4 features a dedicated processor to offload computationally intensive cryptographic algorithms from host applications, reducing the demand on application servers while accelerating overall system performance. Luna PCM 2.4 offers 25 RSA 1024-bit digital signatures per second to meet the needs of all root key management applications.

FIPS 140-2, Level 2

Luna PCM 2.4 is FIPS 140-2, Level 2 validated for environments that require the highest levels of physical and operational security with tamper and intrusion resistance. Each Luna PCM 2.4 token is sealed from physical tampering or modification, and shielded against electronic probing or data recovery techniques to prevent the extraction or compromise of data contained within the token. The Luna PCM 2.4 is also RoHS compliant to meet the material component standards for electrical and electronic equipment established for the European Union market.

Built for HSM Best Practices

HSM Best Practices are the result of collaboration between vendors, auditors, and business process professionals to define duplicable operational standards that apply to system security. HSM Best Practices provide guidelines for the design and operation of HSM products to maintain the highest level of security and assurance. Luna PCM 2.4 maintains security by addressing HSM Best Practices through all aspects of its hardware, software, and operational design.

Full Cryptographic API Support for Easy Integration

Adding hardware security and performance to your applications is easy with Luna PCM 2.4. With support for PKCS#11, Microsoft CryptoAPI, Java JCA /JCE CSP, and Open SSL, Luna PCM 2.4 supports all major Cryptographic APIs to simplify development and speed application deployment. A full SDK toolkit is available for custom development.

Cryptographic Functions include hardware accelerated random number generation (RNG) per Annex A, 2.4 of ANSI X9.31, symmetric and asymmetric key pair generation, hardware-secured key management and storage, hardware-accelerated encryption and decryption, and hardware-accelerated digital signing.

Enterprise Data Protection

SafeNet Luna PCM 2.4 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

Technical Specifications

Operating Systems

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

Cryptographic Performance

- 25 1024-bit RSA digital signatures per second

Cryptographic Algorithms

Asymmetric Key Encryption and Key Exchange

- RSA (512-4096 bit), PKCS #1 v1.5, OAEP PKCS#1 v2.0
- Diffie-Hellman (512-1024 bit)

Suite B Algorithm Support

ECC Support

- ECDSA

Digital Signing

- RSA (512-4096-bit), DSA (512-1024-bit), PKCS #1 v1.5

Symmetric Key Algorithms

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

Hash Digest Algorithms

- SHA-1, MD-2, MD-5, SHA256, SHA512, SHA-224, SHA-384

Message Authentication Codes

- HMAC-MD5, HMAC-SHA-1, SSL3-MD5-MAC, SSL3-SHA-1-MAC

ECC Brainpool Curves (named and user-defined)

Object Limit

- 1280 object limit

Regulatory Standards

Certification

- U/L 1950 & CSA C22.2 safety compliant
- FCC Part 15 - Class B
- FIPS 140-2, Level 2
- RoHS compliant
- BAC and EAC ePassport Certification

Physical Characteristics

Connectivity

- Luna CA4 Token - Type II PC Card Interface, 5V (+/- 0.25V)
- Luna Dock Card Reader - 2.0 Full Speed Device, 2 Type II PC Card Slots, 1 PED Port

Temperature

- Operating 0°C to 35°C
- Storage -20°C to +65°C

Dimensions

- Luna CA4 Token - Type II PC Card; 3.38" x 2.12" x 0.18"
- Luna Dock - 8.78" x 6.26" x 2.23"
- 3.82lb
- PED II - 6.65" x 3.95" x 0.83"



www.safenet-inc.com

Corporate Headquarters:

4690 Millennium Drive, Belcamp, Maryland 21017 USA
Tel.: +1 410 931 7500 or 800 533 3958, Fax: +1 410 931 7524,
Email: info@safenet-inc.com

EMEA Headquarters:

Tel.: +44 (0) 1276 608 000, Email: info.emea@safenet-inc.com

APAC Headquarters:

Tel: +852 3157 7111, Email: info.apac@safenet-inc.com

For all office locations and contact information, please visit www.safenet-inc.com/company/contact.asp

©2009 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-Luna PCM 2.4 - 11.13.09