Luna CA4 Root Key Management System

PRODUCT BRIEF

Benefits

- Most Robust Hardware Backup and Physical Security
- FIPS 140-2 Level 3 validated
- Suite B Algorithm Support
- ECC Support
- Easy to Integrate
- Migrate from Luna CA3 to CA4

Luna® CA4 Root Key Management System is a dedicated Hardware Security Module (HSM)designed to provide the highest levels of performance and protection for the cryptographic keys at the heart of today's Public Key Infrastructure (PKI) systems.

Secure Hardware Key Management

Luna CA4 features industry-leading hardware key management. All key materials used by Luna CA4 are maintained exclusively within the confines of Luna CA4's cryptographic hardware: from creation, to storage, to use, and destruction, sensitive cryptographic keys are never exposed outside of Luna CA4.

Hardware Cryptographic Processing

Luna CA4 features a dedicated processor to offload computationally intensive cryptographic algorithm from host applications, reducing the demand on application servers while accelerating overall system performance. Luna CA4 offers 25 RSA 1024-bit digital signatures per second to meet the needs of all root key management applications.

Two-Factor Administrator Authentication

The data contained within an HSM is extremely sensitive - should it fall into the wrong hands, the trust chain upon which a PKI relies is broken and the PKI collapses. To prevent unauthorized administrative and application access, Luna CA4 features dedicated two-factor authentication. To achieve true two-factor, Trusted Path authentication, Luna CA4 includes the Luna PED (PIN Entry Device), a handheld authentication console, and role-splitting PED Keys (small, key-shaped digital identification tokens). Luna CA4 also adds multi-person authentication, whereby multiple people, each possessing a PED Key, are required to authenticate before administration actions can be performed.

FIPS 140-2, Level 3

Luna CA4 is FIPS 140-2, Level 3 validated for environments that require the highest levels of physical and operational security with tamper and intrusion resistance. Each Luna CA4 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 CA4 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 PKI vendors, auditors, and business process professionals to define duplicable operational standards that apply to PKI security. HSM Best Practices provide guidelines for the design and operation of HSM products to maintain the highest level of security and assurance. Luna CA4 maintains security by addressing HSM Best Practices through all aspects of its hardware, software, and operational design.

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 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 3
- 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" at the end of this line plus:
- - 3.82 lb
- - PED II - 6.65" x 3.95" x 0.83"

Full Cryptographic API Support for Easy Integration

Adding hardware security and performance to your applications is easy with Luna CA4. With support for PKCS#11, Microsoft CryptoAPI , Java JCA /JCE CSP, and Open SSL, Luna CA4 supports all major Cryptographic APIs to simplify development and speed application deployment. A full SDK toolkit is available for custom development. Cryptographic Functions include true hardware accelerated random number generation (RNG) per Annex C of ANSI X9.17, symmetric and asymmetric key pair generation, hardware-secured key management and storage.

Integrated with All Major PKI Application Platforms

To provide simplified integration, SafeNet works closely with application partners and resellers to ensure seamless compatibility with all major PKI applications. As the world's most trusted HSM, Luna CA4 supports applications from VeriSign, RSA, Entrust, Microsoft, and more.

Hardware Secured Backup

Storing private keys on traditional backup media like magnetic tape, floppy disks or optical media does not provide security - insecure media can be lost or copied without your knowledge. Luna CA4's hardware key cloning maintains hardware-secured backups and verifiable audits through a direct hardware-to-hardware backup procedure. Luna Key Cloning copies the contents of one secure Luna CA4 cryptographic token to another without exposing the keys outside of the HSM. To prevent unauthorized use of backup materials, backup tokens maintain the same access controls as the original token.

Enterprise Data Protection

SafeNet Luna CA4 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

Ready Entrust

RoHS COMPLIANT

PCI SECURITY VENDOR ALLIANCE

FIPS VALIDATED 140-2

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