

Benefits

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 CA³'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 CA³ 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.

Integrated Physical Security

Luna CA³ is designed to meet stringent FIPS (Federal Information Processing Standards) 140-1, Level 3 and Common Criteria EAL4+ requirements for tamper and intrusion resistance. Each Luna CA³ 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.

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 CA³ supports applications from VeriSign, Entrust, Microsoft, Baltimore, Computer Associates, and more.

Luna CA³

Root Key Management System



Luna[®] CA³ 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 PKI systems.

Secure Hardware Key Management

Luna CA³ features industry-leading hardware key management. All key materials used by Luna CA³ is maintained exclusively within the confines of Luna CA³'s cryptographic hardware: from creation, to storage, to use, and destruction, sensitive cryptographic keys are never exposed outside of Luna CA³.

Hardware Cryptographic Processing

Luna CA³ features a dedicated processor to offload computationally intensive cryptographic chores from host applications, reducing the demand on application servers and accelerating performance. Luna CA³ 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 CA³ features dedicated two-factor authentication. To achieve true two-factor, Trusted Path authentication, Luna CA³ includes the Luna PED (PIN Entry Device), a handheld authentication console, and role-splitting PED Keys (small, key-shaped digital identification tokens). Luna CA³ also adds multi-person authentication, whereby multiple people, each possessing a PED Key, are required to authenticate before administration actions can be performed.

FIPS 140-1, Level 3 and Common Criteria EAL 4+ Validated

Luna CA³ is FIPS 140-1, Level 3 validated and Common Criteria EAL 4+ certified for environments that require the highest levels of physical and operational security.



Built for HSM Best Practices

HSM Best Practices are the result of collaboration between PKI vendors, auditors, and business process professionals to define reproducible 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 CA³ 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 CA³. With support for PKCS#11, Microsoft CryptoAPI, Java JCA /JCE CSP, and Open SSL, Luna CA³ supports all major Cryptographic APIs to simplify development and speed application deployment. A full SDK toolkit is available for custom development.

Cryptographic Hardware Validation is FIPS 140-1, Level 3 - certificate number 214 and Common Criteria (CC) EAL 4+.

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, hardware-accelerated encryption and decryption, and hardware-accelerated digital signing.

Technical Specifications

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)

Digital Signing

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

Symmetric Key Algorithms

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

Hash Digest Algorithms

- SHA-1, MD-2, MD-5

Message Authentication Codes (MAC)

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

Physical Characteristics

Connectivity

- Luna CA³ Token - Type II PC Card Interface, 5V (+/- 0.25V)
- Luna Dock Card Reader - LVDS External Interface via MDR-26 cable (supplied), 2 Type II PC Card Slots, 1 PED Port

Temperature

- Operating 0°C to 50°C (with Luna DOCK)
- Storage -20°C to +65°C

Dimensions

- Luna CA³ Token - Type II PC Card; 53.67 mm x 85.73 mm x 4.64 mm (3.38" x 2.12" x 0.18")
- Luna Dock - 230.53 mm x 147.57 mm x 72.64 mm (9.08" x 5.81" x 2.86")
- 1.7kg (3.82lb)

Regulatory Standards

Certification

- U/L 1950 & CSA C22.2 safety compliant
- FCC Part 15 - Class B
- FIPS 140-1, Level 3
- ISO - 9002 Certification



NORDIC DISTRIBUTOR

PERICO AS

Lilleakerveien 4, Inngang 1A
0283 OSLO
NORWAY

Email: info@perico.no
Tel: +47 22 06 40 50
www.pericosecurity.com

