# Luna® SA HSM

PRODUCT BRIEF

Award winning application protection through powerful cryptographic processing and hardware key management

## Benefits

**Most Secure**

- Includes a FIPS 140-2 Level 3 validated cryptographic module
- Multi-level access control
- Intrusion-resistant, tamper-evident hardware
- Strongest cryptographic algorithm
- Suite B Algorithm Support
- Keys in hardware
- Commom Criteria EAL 4+ Certified

**Performance and Scalability**

- Cryptographic acceleration up to 5,500 transactions per second
- Wide range of configurations
- Software upgradeable
- Up to 20 unique partitions

**Sample Applications**

- PKI key generation and key storage (online CA keys and offline CA keys)
- Certificate validations
- Transaction processing
- Database encryption
- Smart card issuance
- Document signing

## Secure Hardware Key Management and Cryptographic Processing

SafeNet Luna SA HSM is designed to ensure the integrity and security of cryptographic key management, and is unrivalled in its security and cryptographic acceleration of applications. The Luna SA is capable of up to 5,500 transactions per second, and offers optional standalone authentication to protect the most demanding security applications. The FIPS 140-2 validated Luna SA is used by hundreds of businesses and government organizations deploying a cryptographic system for hardware key storage, transactional acceleration, certificate signing, code or document signing, bulk generation or encryption of keys or data. Luna SA's data contents can be securely stored on Backup Tokens to simplify backup, cloning, and disaster recovery. To protect existing HSM investments, SafeNet Luna CA4 cryptographic tokens interoperate with Luna SA through an integrated PC-Card token interface.

## Network Shareable for Easy Deployment

Luna SA includes Ethernet connectivity for flexible deployment and scalability using standard datacom cabling. Built-in support for TCP/IP (Internet Protocol) ensures that Luna SA deploys easily into existing network infrastructures and communicates with other network devices. Multiple application servers can share the Luna SA's cryptographic capabilities through Network Trust Links (NTLS) -up to 800- that combine 2-way digital certificate authentication and 256 bit SSL encryption to secure communication channels (see Figure 1).

## Partitioning and High Availability

Customers implementing the Luna SA enjoy significant cost savings from the Luna SA's partitioning concept for signing/key management. Partitioning splits a single HSM to a maximum of 20 virtual HSMs, each with their own access controls and independent key storage. The Luna SA is available in a PKI bundle, featuring built-in support for a second, PCMCIA-based HSM via the SA's integrated card reader, which is accessible via the same client API as the Luna SA. Enterprises operating the Luna SA with the PKI bundle face significant cost savings as the HSM functionality (key generation/ offline root/online root/key export) is made available using one chassis as opposed to two or three.

For mission-critical applications that require uninterrupted up-time, the Luna SA's High Availability (HA) feature allows multiple Luna SA appliances to be grouped together to form one virtual device. To Clients, the HA Group appears as a single Luna SA. The HA Group technology shares the transaction load, synchronizes data among members of the group, and gracefully redistributes the processing capacity in the event of failure in a member machine, to maintain uninterrupted service to Clients. The Luna SA HA feature provides load-balancing to improve performance and response time while providing availability assurance through redundancy, as well as the ability to easily recover a unit when it returns to service.

## Integration and Remote Administration

Luna SA features the Secure Command Line Interface (SCLI) to simplify remote system administration and streamline maintenance. A local console port is offered for secure initial configuration or direct system administration.

Multi-layered authentication capabilities control access to the Luna SA's administrative functions to provide the highest degree of protection for sensitive cryptographic keys and prevent unauthorized system configuration changes while still permitting flexible remote management and monitoring.

New in version 4.4 is Remote PED (PIN entry device), an authentication device that connects to a remote Windows workstation via USB, and communicates over a secure network connection to

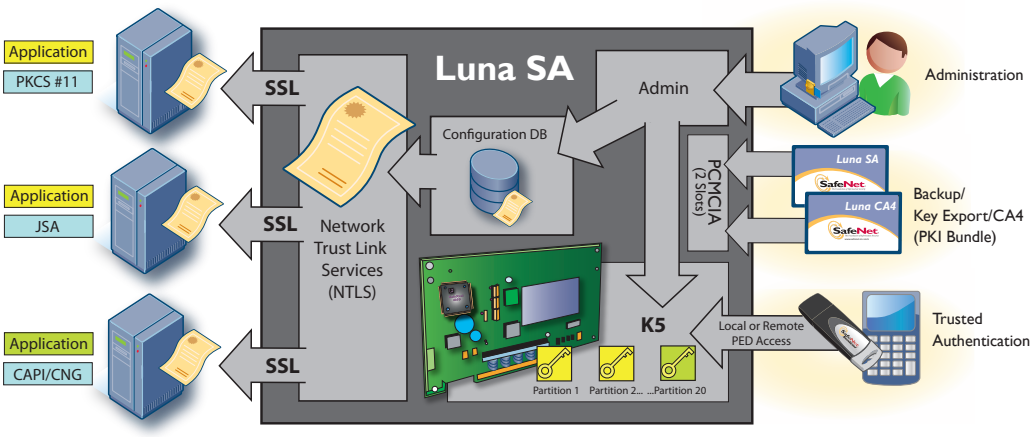


*Figure 1*

a Luna SA. Full PED functionality facilitates management of security administration functions by offering the security administrator to centrally manage administration rights remotely by simply inserting the required key, and entering the secret PIN into the PED.

## Standard Cryptographic API Support for Easy Integration

Luna SA is compatibile with; PKCS#11, CAPI (Microsoft CryptoAPI 2.0), JCA (Java Cryptographic Architecture), OpenSSL, and dual support of Microsoft CryptoAPI 2.0 and Microsoft CNG cryptographic APIs.

## Third Party Validations

SafeNet Luna SA meets or exceeds the best practice security requirements set forth by numerous legal and regulatory requirements. It contains a FIPS 140-2 validated cryptographic module and is Common Criteria EAL 4+ certified. Industry standards such as PCI-DSS, HIPAA, National Security Suite B algorithms, DNSSEC and numerous ISO standards, to name a few, can be quickly and easily implemented using SafeNet Luna SA HSMs.

## Software Upgradeable

Luna SA uses SafeNet's extensible Ultimate Trust Security Platform to add new functionality or increase performance. With PKI-validated software upgrades, new software features can be added as they are developed, or existing configuration features can be easily deployed to units in the field.

## Enterprise Data Protection

SafeNet HSMs are a key component of SafeNet's comprehensive Enterprise Data Protection (EDP) solution to reduce the cost and complexity of regulatory compliance, data privacy, and information risk management. SafeNet EDP is the only solution that secures data across the connected enterprise, from core to edge, providing 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.

RoHS COMPLIANT

PCI SECURITY VENDOR ALLIANCE

FIPS VALIDATED 140-2 inside

## Technical Specifications

### Operating System
- Windows 2000, 2003, 2008
- Solaris 9, 10 (SPARC and x86)
- Linux RedHat Enterprise 4,5
- AIX 5.3
- HP-UX 11i (PA-RISC and Itanium)
- VM Ware

### Cryptographic APIs
- PKCS#11, Microsoft CAPI, and CNG
- JCA/JCE

### Cryptographic Functions
- True hardware accelerated random number generation (Annex C of ANSI X9.17)
- Symmetric and asymmetric key pair generation
- Encryption and decryption
- RSA
- Digital signing

### Cryptographic Algorithms
- Asymmetric Key with Diffie-Hellman (1024-4096 bit), RSA (512-4096 bit) and (PKCS#1 v1.5, OAEP PKCS#1 v2.0), Digital Signing via RSA (1024-4096-bit), DSA (512-1024-bit), (PKCS#1 v1.5) and Symmetric Keys through 3DES, (double & triple key lengths), AES, RC2, RC4, RC5, CAST-128. Hash Digest is SHA-1, SHA-2 (160, 256, 512), MD-5 and Message Authentication Codes (MAC) are HMAC-MD5, HMACSHA-1, SSL3-MD5-MAC, SSL3-SHA-1-MAC Eliptical Curve Cryptography (ECC) Korean Algorithms. ECC Brainpool Curves (named and user-defined), Suite B Algorithm Support and ARIA support

### Physical Characteristics
*Connectivity*
- 2x 10/100 Ethernet, CAT5, UTP
- Up to 800 NTLS
- Luna PED authentication port
- Local serial console port
- Luna Token PC-Card slot

*Dimensions*
- 1U rackmount chassis
- 19.0" x 20.6" x 1.725"
- 35lb (15.9kg)

*Removable Storage*
- PC Card Type II Slot

*Temperature*
- Operating 0°C – 35°C, Storage -20°C – +65°C

*Power Requirements*
- 1.5A@120V Max

### Regulatory Standards
- U/L 1950 (EN60950) & CSA C22.2 compliant
- FCC Part 15 - Class B
- FIPS 140-2, Level 3 validated
- RoHS compliant
- BAC and EAC ePassport Certification
- Commom Criteria EAL 4+ Certified

SafeNet®
The Foundation of Information Security
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


PB-Luna SA 4.4-11.25.09