

Luna[®] SA 4.3

Network-Attached Hardware Security Module

A flexible, network-attached hardware security module featuring powerful cryptographic processing and hardware key management for applications where security and performance are the priority.



Benefits

Most Secure

- FIPS 140-2 Level 3 validated Multi-level access control
 - Intrusion-resistant, tamper-evident hardware
- Strongest cryptographic algorithm
 - Suite B Algorithm Support
 - Keys in hardware

Performance and Scalability

- Cryptographic acceleration up to 4,000 transactions per second
- Wide range of configurations
 - Software upgradeable
- Up to 20 unique partitions

Sample Applications

- PKI key generation and storage
 - Root key protection
 - Database encryption
 - Certificate validations
 - Smart card issuance
 - Document signing

Secure Hardware Key Management and Cryptographic Processing

Luna SA features an integrated hardware security module (HSM) offering hardware key management and cryptographic acceleration for unrivalled security and performance. Luna SA 4.3 HSM is capable of up to 4,000 transactions per second*. Twice as fast as the competition, and offers optional standalone authentication to protect the most demanding security applications.

Network Shareable

Luna SA includes Ethernet connectivity for flexible deployment 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 (up to 800 NTLS) that combine 2-way digital certificate authentication and 128-bit SSL encryption to secure communication channels between the Luna SA and application servers, ensuring that sensitive data remains protected in transit.

Configuration Flexibility

Luna SA's flexible feature set is available to solve a wide variety of security problems. Luna SA's HSM Partitioning allows a single HSM to be divided into multiple logical HSM partitions. Luna SA is available with up to 20 unique HSM Partitions, each with their own access controls and independent key storage. Luna SA supports load-sharing and High Availability by allowing multiple units to operate in parallel to dramatically reduce the risk of a service outage, as well as increased performance and throughput.

Multi-Level Access Control and Authentication

Multi-level authentication policies 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. Access to sensitive HSM administration functions is controlled through the Luna PED II (PIN Entry Device), a handheld, two-factor authentication device connected directly to the Luna SA.

Standard Cryptographic API Support for Easy Integration

Luna SA models simplify integration and ensures application compatibility 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.

Integrated Physical Security

Tamper-evident seals, intrusion detection switches, and shielded connectors designed into the Luna SA minimize exposure to direct physical attacks.

Simplified 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.

Backup and Disaster Recovery

Luna SA's data contents can be securely stored on Backup tokens to simplify backup, cloning, and disaster recovery.





FIPS 140-2 Level 3 Validated	✓
RoHS Compliant	✓
1U Rackmount Chassis	✓
Transactions Per Second	4000**
Cryptographic APIs	
PKCS#11	✓
Microsoft CAPI v2.0	✓
JCA	✓
JCE	✓
OpenSSL	✓
Luna PED	✓
Luna PEDII	✓
Front-Panel System Status Indicator	✓

* Luna SA 3.x 2Us are upgradeable to the Luna SA 4.3 functionality

** Performance 4000s/s1, 2• 1 – based on uncongested network transacted operations 2 – devices must be running version 4.3 of software or later

Luna Token Interoperability

To protect existing HSM investments, SafeNet Luna CA4 cryptographic tokens interoperate with Luna SA through an integrated PC-Card token interface.

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. Customers with an existing Luna SA appliance can upgrade to the 4.3 software on their existing unit or can purchase the new Luna SA 4.0 unit and migrate their existing Luna PED Keys to the new style Luna PED II iKeys. Existing customers can also purchase a new Luna PED II for use on previous Luna SA versions.



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

©2008 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-HSM SA 4.3-06.10.08

Technical Specifications

Operating System

- Windows 2000, 2003, 2008
- Solaris 8, 9, 10 (SPARC and x86)
- Linux RedHat Enterprise 3, 4, 5
- AIX 5.2, 5.3
- HP-UX 11i (PA-RISC and Itanium)

Cryptographic APIs

- PKCS#11, Microsoft CAPI, and CNG

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 Elliptical 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

- UL 1950 (EN60950) & CSA C22.2 compliant
- FCC Part 15 - Class B
- ISO - 9002 Certification
- FIPS 140-2, Level 3 validated
- RoHS compliant
- BAC and EAC ePassport Certification