

Benefits

Security

The Luna SA's operational, software, and hardware design ensure that the integrity and security of cryptographic processes and key management with multiple levels of security.

Operational controls, including optional two-factor authentication and per-process software access, prevent unauthorized access and administration. Secure software practices maintain system integrity with Secure Boot verification and PKI-signed code modules to prevent the introduction of rogue software into the Luna SA. The Luna SA's intrusion-resistant, tamper-evident seals include anti-tamper screws, probe-resistant baffles, and intrusion detection switches to provide both passive and active defense against attack.

Validations

The Luna SA 4.0 is available in two separate versions for FIPS validation and RoHS compliancy. The FIPS 140-2 validated HSM version protects critical cryptographic keys and accelerates sensitive cryptographic operations across a wide range of security applications. FIPS 140-2 Level 3 and FIPS 140-2, Level 2 variants are available to match the security profile of your specific application.

The RoHS compliant HSM version meets the material component standards for electrical and electronic equipment established for the European Union market.

Scalable

With a wide range of configuration options, the Luna SA scales to meet your demands as applications grow. Core configuration parameters are upgradeable via software, allowing the Luna SA to scale without the necessity to replace hardware.

Luna[®] SA 4.0

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.



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 4.0 HSM is capable of up to 7,000 transactions per second. The fastest in the industry. And, offers optional standalone authentication to protect the most demanding security applications.

Network Shareable

The 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 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. The 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.



FIPS 140-2 Validated	✓	In Progress
RoHS Compliant		✓
2U Rackmount Chassis	*✓	
1U Rackmount Chassis		
Transactions Per Second	> 1200	3000/7000**
Cryptographic APIs		
PKCS#11	✓	✓
Microsoft CAPI v2.0	✓	✓
JCA	✓	✓
JCE	✓	✓
OpenSSL	✓	✓
Luna PED	✓	✓
Luna PEDII		✓
Key Import of Private RSA Keys		✓
Front-Panel System Status Indicator		✓

*The Luna SA 3.x 2Us are upgradeable to the Luna SA 4.0 functionality

**To be determined

Standard Cryptographic API Support for Easy Integration

The Luna SA models simplify integration and ensures application compatibility with; PKCS#11, Microsoft CryptoAPI 2.0, JCA (Java Cryptographic Architecture), JCE (Java Cryptographic Extensions), and OpenSSL 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

The 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.



NORDIC DISTRIBUTOR

PERICO AS

Lilleakerveien 4, Inngang 1A
0283 OSLO
NORWAY

Email: info@perico.no

Tel: +47 22 06 40 50

www.pericosecurity.com

Backup and Disaster Recovery

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

Luna Token Interoperability

To protect existing HSM investments, SafeNet Luna CA3 cryptographic tokens interoperate with the Luna SA through and integrated PC-Card token interface

Software Upgradeable

The 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 4.0 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.

Technical Specifications

Operating System

- Windows 2000, 2003, XP
- Solaris 8, 9, 10
- Linux (Red Hat 8)
- Linux (Enterprise 3)
- AIX (5.1, 5.2, 5.3)
- HP-UX 11i

Cryptographic APIs

- PKCS#11 v2.01
- Microsoft CAPI v2.0,
- JCA (Java Cryptographic Architecture)
- JCE (Java Cryptographic Extensions)
- OpenSSL

Cryptographic Hardware Validation

- RoHS compliant

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 Performance

Luna SA 3.0 — Over 1200 1024-bit RSA cryptographic operations per second
Luna SA 4.0 — Over 7000 tps

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

Physical Characteristics

Connectivity

- 2x 10/100 Ethernet, CAT5, UTP
- Luna PED authentication port
- Local serial console port
- Luna Token PC-Card slot

Dimensions

- 1U full-length 19" rackmount chassis (Luna SA 4.0 model) (ANSI/EIA-310-D compliant)
- 19.0" x 20.6" x 1.725"

Removable Storage

- PC Card Type II Slot, 5V (+/- 0.25V)

Temperature

- Operating 0°C – 40°C, Storage -20°C – +65°C

Power Requirements

- 1.5A@120V Max

Regulatory Standards

Certification

- U/L 1950 (EN60950) & CSA C22.2 compliant
- FCC Part 15 - Class B
- ISO - 9002 Certification

