Luna SA 5.0 Hardware Security Module

PRODUCT BRIEF

Benefits & Features

Most Secure

- Secure transport mode for high-assurance delivery
- Multi-level access control
- Multi-part splits for all access control keys
- Intrusion-resistant, tamper-evident hardware
- Strongest cryptographic algorithms
- Suite B algorithm support
- Keys in hardware including network trust link
- HSM decommission button

Performance and Scalability

- Cryptographic acceleration up to 6,000 1024-bit RSA tps; 400 384-bit ECC tps
- Wide range of configurations
- Field-upgradeable memory expansion
- Software upgradeable
- Up to 20 unique partitions
- Dual, hot-swappable power supply ensuring consistent performance and no down-time

Sample Applications

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

Luna SA 5.0 is the choice for enterprises requiring strong cryptographic security for paper-to-digital initiatives, digital signatures, DNSSEC, hardware key storage, transactional acceleration, certificate signing, code or document signing, bulk key generation, data encryption, and more.

A Unique Design Philosophy

By its very name, HSM implies hardware. As such, most security professionals assume that all HSMs actually store cryptographic keys in hardware, as Luna SA does by default. In fact, while other leading HSMs generate their keys in hardware, they actually store the cryptographically wrapped keys on an application server. These keys, residing in software, can be easily detected—creating an additional attack surface.

The advantages of hardware are key reasons why the world's largest enterprises and government organizations trust SafeNet HSMs to guard more digital identities and interbank fund transfers than any other HSM in the world.

With Luna SA 5.0, SafeNet is going deeper into hardware than ever before, incorporating an HSM within an HSM, by utilizing a special, SafeNet-designed, tamper-proof ASIC cryptographic processor. This chip leverages the same technology that is protecting the most sensitive data in space, data centers, and defense facilities. In addition, with Luna SA 5.0, more keys may be stored in hardware than ever before.

Secure Hardware Key Management and Cryptographic Processing

SafeNet Luna SA HSM ensures the integrity and security of cryptographic operations in a robust, high-availability appliance. Luna SA is capable of up to 6,000 RSA and 400 ECC transactions per second and offers optional standalone authentication to protect the most demanding security applications.

Partitioning, High Availability and Secure Backup

Significant cost savings are possible with the Luna SA partitioning capability 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. Luna SA is available in a PKI bundle, featuring support for SafeNet's Luna Dock 2 PCMCIA card reader and tokens, accessible via the same client API as Luna SA (see figure 1). Operating Luna SA with the PKI bundle drastically reduces cost as the HSM functionality (key generation/offline root/online root/key export) is available using one chassis as opposed to two or three.

Luna SA's High Availability (HA) feature allows multiple Luna SA appliances to be grouped together to form one virtual device. The HA Group technology shares the transaction load, synchronizes data among members of the group, and redistributes the processing capacity in the event of failure in a member machine to maintain uninterrupted service to up to 100 clients. The HA capability also enables easy recovery when a unit returns to service.

Technical Specifications

Operating System
- Windows Server 2003, 2008 R2; Solaris 9 (SPARC), 10 (SPARC & x86); Linux E4, E5;SuSE 10, 11; AIX 5.3, 6.1; HP-UX 11i (PA-RISC & Itanium); VM Ware

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

Cryptographic Functions
- FIPS 140-2 approved DRBG (SP 800-90 CTR mode)
- RSA, DSA and ECDSA signing

Cryptographic Algorithms
- Full Suite B support
- Asymmetric Key with Diffie-Hellman (1024-4096 bit), RSA (1024-8192 bit) & (PKCS#1 v1.5, OAEP PKCS#1 v2.0), Digital Signing via RSA (1024-8192 bit), DSA (1024 & 2048 bit), (PKCS#1 v1.5) & Symmetric Keys through 3DES, (double & triple key lengths), AES, RC2, RC4, RC5, CAST-128. Message Digest is SHA-1, SHA-224, SHA-256, SHA-384 & SHA-512, MD-5 & MAC are HMAC-MD5, HMAC SHA-1, SSL3-MD5-MAC, SSL3-SHA-1-MAC, Elliptic Curve Cryptography (ECC), Korean Algorithms. ECC Brainpool Curves (named & user-defined)

Certifications
- U/L 1950 (EN60950) & CSA C22.2
- FCC Part 15 - Class B
- RoHS
- BAC & EAC

Physical Characteristics

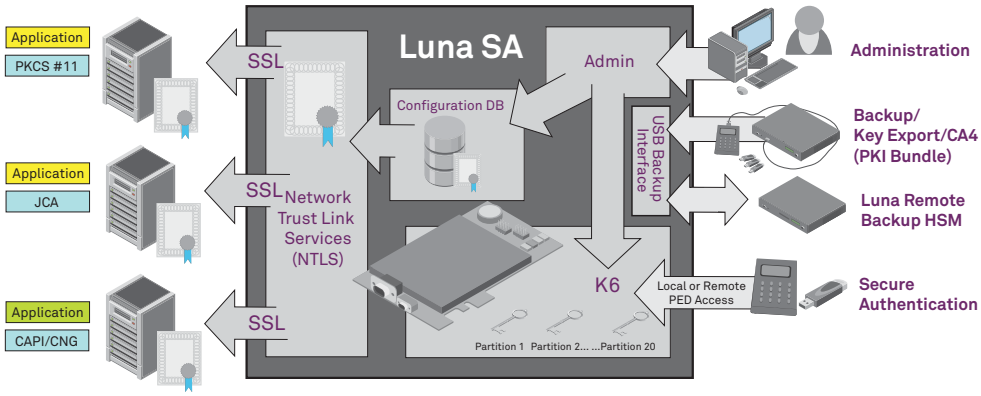
Connectivity
- 2x 10/100/1000 Ethernet, CAT5, UTP
- Up to 800 simultaneous NTLS connections
- Luna PED authentication port
- Local serial console port
- Luna Token PC-Card reader and/or G5 connection via USB

Dimensions
- 1U rack mount chassis
- 19.0" x 21" x 1.725"
- 28lb (12.7kg)

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

Power Requirements
- Input: 100-240Vac 50-60Hz 8-4A

Luna SA's data contents can be securely stored on devices to simplify backup, duplication, and disaster recovery. Luna SA includes a remote backup feature to allow administrators to securely move copies of their sensitive cryptographic material to other HSM devices, most notably SafeNet's Luna Backup HSM (see Figure). With a single SafeNet Luna Backup HSM, an administrator can backup and restore keys to and from up to 20 Luna SA HSMs.



Ease of Integration, Administration, and Management

For ease of integration, Luna SA standard cryptographic API support is compatible with PKCS#11, CAPI (Microsoft CryptoAPI 2.0), CNG (Microsoft Cryptography API: Next Generation), JCA (Java Cryptographic Architecture) and OpenSSL.

In addition, organizations can eliminate costs accrued from sending personnel to remote data centers for HSM administration operations. With the SafeNet Remote PED II, 1) keys are generated in the HSM, 2) the HSM is configured to enable secure transport, and 3) the HSM is "racked and stacked" at the data center for remote and secure initialization of the device.

Luna SA features a Secure Command Line Interface (SCLI) to simplify system administration and streamline maintenance. A local console port and remote administration offers 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 management and monitoring.

Luna SA offers software upgradeability using SafeNet's extensible Ultimate Trust Security Platform to add new functionality or increase performance. With PKI-validated software upgrades, organizations can add new software features as they are developed, or deploy existing configuration features to units in the field with ease.

Network Shareable for Easy Deployment

Ethernet connectivity enables flexible deployment and scalability. Built-in TCP/IP support 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 two-way digital certificate authentication and 256-bit SSL encryption to secure communication channels (see Figure 1).

RoHS COMPLIANT

Microsoft GOLD CERTIFIED Partner

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