SafeNet | THE DATA PROTECTION COMPANY

Luna SA

Hardware Security Module

PRODUCT BRIEF

Benefits & Features

Most Secure

- Keys in hardware
- Remote Management
- Secure transport mode for high-assurance delivery
- Multi-level access control
- Multi-part splits for all access control keys
- Intrusion-resistant, tamper-evident hardware
- Suite B algorithm support
- Secure decommission
- Secure Audit Logging
- Strongest cryptographic algorithms

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 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, 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, more keys may be stored in hardware than ever before.

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. The optional SafeNet Luna SA PKI bundle drastically reduces cost as HSM functionality (key generation/offline root/online root/key export) is possible using one device 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.

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. With a single SafeNet Luna Backup HSM, an administrator can backup and restore keys to and from up to 20 Luna SA HSMs.

Technical Specifications

Operating System
- Windows, Linux, Solaris, AIX, HP-UX
- Virtual: VMware, Hyper-V, Xen

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

Cryptography
- Full Suite B support
- Asymmetric: RSA (1024-8192), DSA (1024-3072), Diffie-Hellman, KCDSA, Elliptic Curve Cryptography (ECDSA, ECDH, ECIES) with named, user-defined and Brainpool curves
- Symmetric: AES, RC2, RC4, RC5, CAST, DES, Triple DES, ARIA, SEED
- Hash/Message Digest/HMAC: SHA-1, SHA-2 (224-512), SSL3-MD5-MAC, SSL3-SHA-1-MAC
- Random Number Generation: FIPS 140-2 approved DRBG (SP 800-90 CTR mode)

Physical Characteristics
- Standard 1U 19in. rack mount chassis
- Dimensions: 19" x 21" x 1.725" (482.6mm x 533.4mm x 43.815mm)
- Weight: 28lb (12.7kg)
- Input Voltage: 100-240V, 50-60Hz
- Power Consumption: 180W maximum, 155W typical
- Temperature: operating 0°C – 35°C, storage -20°C – 60°C
- Relative Humidity: 5% to 95% (38°C) non-condensing

Security Certifications
- FIPS 140-2 Level 2 and Level 3
- Common Criteria EAL4+**
- BAC & EAC ePassport Support

**Under evaluation

Safety and Environmental Compliance
- UL, CSA, CE
- FCC, KC Mark, VCCI, CE
- RoHS, WEEE

Host Interface
- Dual Gigabit Ethernet ports

Reliability:
- Mean Time Between Failure (MTBF) 66,561 hrs

The World's Only Crypto Hypervisor Ready Hardware Security Module

The SafeNet Crypto Hypervisor represents the first platform that offers all the traditional security benefits of an HSM, while being fully aligned with the dynamic, agile, and elastic nature of cloud and virtualized environments. Luna SA HSM is purposefully designed to support the scalability, performance, availability, and security requirements of the Crypto Hypervisor, and is the only Crypto Hypervisor-ready hardware security module in available in the market today.

Security Audit Logging

Luna SA can be configured to selectively log HSM events for security auditing purposes. This allows for separation of duties between an Audit Officer/Team and the people (e.g., HSM administrator, crypto officer, and crypto user) they are auditing – preventing both the administrative and user personnel from tampering with the log files and the auditors from doing anything administrative or accessing keys. Each log entry originates from the in the HSM and contains when, who, what, and the result of every logging event.

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.

Secure Client to HSM Binding for the Cloud with Host Trust Links

Host Trust Links are an innovative one-time token solution that ensures control over client connections in a virtual environment and enhances connection control in traditional client-server environments. Host Trust Links prevent cloned VM images from establishing a connection to the Luna SA and provide protection against cloning attacks after the VM binding has been established in a running VM instance.

Available in Two Performance Models

Luna SA is available in two performance models; Luna 7000 and Luna SA 1700. Luna SA 7000 is a high performance HSM capable of best in class performance across a breadth of algorithms including ECC, RSA, and symmetric transactions. Luna SA 7000 also features a dual, hot-swappable power supply that ensures consistent performance and no down-time. The low performance variant, Luna 1700, includes a single power supply, and is capable of 1700 RSA 1024-bit transactions per second.

Algorithm	Model	
	Luna SA 1700	Luna SA 7000
RSA-1024	1,700	7,000
RSA-2048	350	1,200
ECC P256	500	1,000
ECIES	200	300
AES-GCM	3700	3700

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