SITEPRO

gemalto
security to be free

PRODUCT BRIEF

SafeNet Network HSM

(Formerly SafeNet Luna SA)

The SafeNet Network HSM from Gemalto is the choice for enterprises requiring strong security for digital signatures, cryptographic key storage, transactional acceleration, certificate signing, code signing, bulk key generation, data encryption, DNSSEC, and more.

Approach to Key Security: Keys in Hardware

SafeNet Network HSM is the most trusted general purpose HSM on the market in part because of its unique approach to protecting cryptographic keys. Unlike other methods of key storage which move keys outside of the HSM into a "trusted layer," the keys-in-hardware approach protects the keys throughout their lifecycle within the FIPS 140-2 validated confines of the SafeNet HSM. This method ensures that your keys always benefit from both physical and logical protections of the Network HSM and reduces your audit burden.

The Leading Hardware Security Module for the Cloud

The latest release of SafeNet Network HSM builds on our leadership in the cloud. A single SafeNet Network HSM can be separated into 100 cryptographically isolated partitions, with each partition functioning as if it was an independent HSM. This provides a tremendous amount of scalability and flexibility, as a single HSM can protect the cryptographic keys of hundreds of independent applications concurrently. What's more, the ability to assign a unique Partition Security Officer to each partition means the configurations of partitions and control over cryptographic keys can be strictly enforced, even in public cloud environments. For service providers, this means partitions can be offered as rentable services and your customers can maintain the trust and confidence that only they have access to their partition and sensitive cryptographic keys.

Flexible Backup and Disaster Recovery Options

SafeNet Network HSM provides secure, auditable and flexible options to simplify backup, duplication, and disaster recovery. Key backups can be performed locally or remotely to a SafeNet Backup HSM, Small Form Factor SafeNet eTokens or other SafeNet HSMs.

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)
- HSM-as-a-Service for private and public cloud environments
- Certificate validation & signing
- Code signing
- Document signing
- Transaction processing
- Database encryption
- Smart card issuance
- Hardware root of trust for the Internet of Things

Secure Audit Logging

SafeNet Network HSM 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 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.

Operational Enhancements

The enhanced SNMP trap functionality of SafeNet Network HSM provides operations teams with real-time visibility into important events related to their HSM infrastructure. Support for the leading Security Information and Event Management (SIEM) platforms enables deeper analysis and streamlined reporting of HSM events.

Common Architecture

All SafeNet general purpose hardware security modules benefit from a common architecture where the supported client, APIs, algorithms, and authentication methods are consistent across the entire general purpose product line. This eliminates the need to design applications around a specific HSM, and provides the flexibility to move keys from form factor to form factor.

Available in Two Performance Models

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

Algorithm	Model	
	Network HSM 1700	Network HSM 7000
RSA-1024	1,700	7,000
RSA-2048	350	1,200
ECC P256	570	2,000
ECIES	200	300
AES-GCM	3600	3600

Technical Specifications

Operating System
- Windows, Linux, Solaris, AIX, HP-UX
- Virtual: VMware, Hyper-V, Xen
- Cloud: AWS, SoftLayer, Azure, vCloudAir

SIEM Integrations
- Splunk, Qradar, Arcsight

API Support
- PKCS#11, Java (JCA/JCE), Microsoft CAPI and CNG, OpenSSL, REST

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, SM3
- 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
- FIPS 186-4
- NIST SP800-131A
- UK AMI Spec Compliance
- Common Criteria EAL4+
- BAC & EAC ePassport Support

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