Luna G5
Hardware Security Module (HSM)
PRODUCT BRIEF

Benefits
- High Assurance HSM Design
- Secure Authentication and Access Control
- Full Cryptographic API Support and Developer Toolkits for Easy Integration
- Fail Safe Security Architecture
- Defense-in-depth Internal Key Hierarchy
- Improved Tamper Detection and Response
- Optimized for Suite B Performance
- Factory Installed ECC Digital ID

Features
- Backup through Luna Key Cloning
- Suite B Support
- M of N per role
- Support for NIST and Brainpool ECC Curves
- User-specified ECC parameters
- Korean algorithm support
- FIPS Compliant RNG
- Common Criteria EAL 4+ in process
- Secure Transport Mode

The Luna G5 is widely used by governments, financial institutions and large enterprises for data, applications and digital identities to reduce risk and ensure regulatory compliance.

Background
In today's digital world, cryptographic keys protect the most confidential data of enterprises, banks and governments. The keys themselves must be strongly protected to ensure their secrecy and authenticity so that information passing through the online infrastructure is not exposed to unauthorized parties. Public Key Infrastructures (PKIs) are commonly employed to properly manage the large number of keys required in a typical enterprise or electronic commerce scenario. PKIs need the highest security available to protect their own cryptographic keys, known as the root keys. SafeNet Hardware Security Modules (HSMs) secure keys within the hardware appliance 100% of time, from key creation, to storage, to use, and to destruction. Maintaining keys in hardware throughout their life-cycle is a best practice mandated by system security auditors and certification bodies responsible for attesting to the security status of PKI systems.

The SafeNet G5 HSM builds upon the Luna product family's long standing industry validated security capabilities and introduces a new design generation to the SafeNet HSM family. The new design directly connects the HSM to the application server via a USB interface.

Convenient and Secure Form Factor
Luna G5 delivers industry leading key management in a portable appliance. All key materials are maintained exclusively within the confines of the hardware. The small form-factor and on-board key storage sets the product apart, making it especially attractive to customers who need to physically remove and store the small appliance holding PKI root keys.

Secure Hardware Key Management
Luna HSMs provide secure hardware key generation, storage, and backup in a range of models and configurations, offering a wide selection of security, and operational capabilities. The Luna G5 version of SafeNet's HSM family of products provides an additional layer of hardware-based key management. At its core is the SafeXcel 3120, a robust, fail safe security system on a chip to protect internal keys and sensitive data. This defense-in-depth security-system-on-a-chip architecture isolates plaintext key material from the HSM's primary firmware by further encrypting internal keys with a key that exists only in the SafeXcel hardware.

Split key techniques provide an enhanced tamper response feature triggered by the detection of external attack or an internal hardware anomaly. This High Assurance design also includes tamper recovery role and secure transport mode (refer to the dedicated section below).

Luna G5 is securely packaged to meet the most stringent requirements for tamper and intrusion resistance.

Technical Specifications

Client API Support
- PKCS#11 v2.20
- Microsoft CryptoAPI (CAPI)
- Microsoft Crypto API: Next Generation (CNG)
- Java JCA/JCE
- OpenSSL

Operating System Support
- Windows, Linux

Cryptographic Processing

Asymmetric Key Transport and Key Exchange:
- RSA (1024-4096 bit), PKCS #1v1.5, OAEP PKCS#1 v2.0,
- Diffie-Hellman (DH) (1024 bit)
- Elliptic Curve Diffie-Hellman (ECDH) (numerous curves supported)

Digital Signing and Verification
- RSA (1024-4096-bit), DSA 1024-bit), PKCS#1 v1.5, ECDSA (numerous curves supported), KCDSA

ECC Support
- ECDSA, ECDH
- Numerous curves supported including NIST P-curves up to P-521, Brainpool Curves, and user-defined curves.

Symmetric Key Algorithms
- TDES (double & triple key lengths), RC4, RC5, AES, SEED, ARIA

Message Digest Algorithms
- SHA-1, HAS-160, SHA224, SHA256,SHA384, SHA512

Message Authentication Codes
- HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512, SSL3-SHA-1-MAC

Suite B Algorithm Support
- AES-128, AES-256
- ECDSA P-256, P-384
- ECDH P-256, P-384
- SHA-256, SHA-384

Random Number Generation
- AES-DRBG compliant with NIST SP 800-90

Compliance Certifications
- FIPS 140-2 Level 2 and Level 3 validation (in process)
- BAC and EAC ePassport
- RoHS

Interface Compatibility
- High Speed USB 2.0 device

Physical dimensions
- 17cm (deep) x 21.5cm (wide) x 4.3cm (high)

Fail Safe Security Architecture

The Luna G5 has an improved internal security architecture that provides an unprecedented level of security for the keys and sensitive data generated, used, and stored in the HSM. Central to this architecture is the SafeXcel-3120 which performs all of the cryptographic operations for NIST-approved algorithms (including Suite B). Modeled after the High Assurance chips that SafeNet develops today, the SafeXcel-3120 acts as the trust anchor and utilizes a secure boot process to ensure only trusted firmware runs within the HSM. In addition to its previously described key management role, the SafeXcel-3120 performs all key generation for NIST-approved algorithms and is used for signing, verification, encryption, and decryption in medium performance environments.

Tamper Recovery Role

The Luna G5 features sophisticated tamper detection and response circuitry to automatically zeroize internal keys in the event of an attempted attack on the HSM. Balancing this extreme security posture with end user ease of use concerns, the Luna G5 includes a capability for properly authenticated security officers to recover from an inadvertent tamper event and quickly put the HSM back into its usable state without the loss of any keys or sensitive data.

Secure Transport Mode

The G5 tamper response circuits have also allowed the introduction of a secure transport mode. Security Officers use the device's tamper recovery role keys to cryptographically lock down the HSM prior to transporting the device. The recovery role keys can be shipped separately and re-combined at the destination to cryptographically verify the HSM's integrity.

Trusted Path Authentication – Locally Connected PED

To prevent unauthorized access to sensitive cryptographic material, Luna G5 offers strong two-factor authentication and multiple administrator roles (now including M of N capabilities for every role). Luna G5 also offers true Trusted Path Authentication using the Luna PED (PIN Entry Device) which is an integrated handheld authentication console that does not rely on commercial keyboards or displays for administrator PIN entry.

Cryptographic Capabilities

Luna G5 supports a broad range of asymmetric key encryption and key exchange capabilities, as well as support for all standard symmetric encryption algorithms. It also supports all standard hashing algorithms and message authentication codes (MAC). The Luna G5 has a hardware implemented random number generator (AES-DRBG) compliant with NIST SP 800-90.

Enhancing the previous generation HSM's support of factory generated digital IDs based on RSA key pairs, the Luna G5 also supports ECC key pairs for use in Suite B applications that require a permanent, factory generated digital ID.

About SafeNet

Founded in 1983, SafeNet is a global leader in information security. SafeNet protects its customers' most valuable assets, including identities, transactions, communications, data, and software licensing, throughout the data lifecycle. More than 25,000 customers across both commercial enterprises, and government agencies, and in over 100 countries, trust their information security needs to SafeNet.

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

©2011 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 (EN)-03.31.11