gemalto
security to be free

PRODUCT BRIEF

SafeNet USB HSM

(Formerly SafeNet Luna G5)

> 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.

The SafeNet USB HSM from Gemalto is a small form factor HSM that is widely used by governments, financial institutions and large enterprises as a hardware cryptographic root of trust for data, applications and digital identities to reduce risk and ensure regulatory compliance.

SafeNet USB HSM Overview

SafeNet USB HSM 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 offline key storage capability sets the product apart, making it especially attractive to customers who need to physically remove, transport and store the small appliance holding PKI root keys.

Cryptographic Capabilities

SafeNet USB HSM 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 SafeNet USB HSM 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 SafeNet USB HSM also supports ECC key pairs for use in Suite B applications that require a permanent, factory generated digital ID.

Algorithm	Model
	SafeNet USB HSM
RSA-1024	200
RSA-2048	63
ECC P256	43
ECIES	20
AES-GCM	71

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
- Secure Audit Logging
- Strongest cryptographic algorithms
- Suite B algorithm support
- Secure decommission

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

Tamper Recovery Role

The SafeNet USB HSM 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 SafeNet USB HSM 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 SafeNet USB HSM 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.

Common Architecture

SafeNet General Purpose HSMs benefit from a common architecture where the supported client, APIs, algorithms, and authentication methods are consistent across the entire general purpose HSM 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.

Technical Specifications

Operating System Support

> Windows, Linux

Client

> Universal SafeNet Client

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

> Dimensions: 8.5" x 6.675" x 1.7" (215.9mm x 169.545mm x 43.18mm)

> Weight: 3.3lb (1.5kg)

> Input Voltage: 100-240V, 50-60Hz

> Power Consumption: 26W maximum, 20W typical

> Temperature: operating 0°C – 35°C, storage -20°C – 70°C

> Relative Humidity: 20% to 95% (38°C) non-condensing

Security Certifications

> FIPS 140-2 Level 2 and Level 3

> BAC & EAC ePassport Support

Safety and Environmental Compliance

> UL, CSA, CE

> FCC, KC Mark, VCCI, CE

> RoHS, WEEE

Host Interface

> USB 2.0

Reliability

> MTBF 124,780 hrs

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

Follow Us: data-protection.safenet-inc.com

GEMALTO.COM

gemalto
security to be free