Trusted Cyber Technologies

Luna G5 for Government
USB-Attached HSM

The Luna G5 for Government is a small form factor HSM that is widely used by government agencies for data, applications and digital identities to reduce risk and ensure regulatory compliance. Derived from industry leading technology, the Luna G5 for Government is manufactured, sold, and supported exclusively by Thales Trusted Cyber Technologies (TCT).

Luna G5 for Government Overview

Luna G5 for Government delivers industry leading key management in a small and portable form factor. All key material is 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 with business critical keys that need to physically detach and store the HSM in a secure offline environment.

Tamper Recovery Role

The Luna G5 for Government 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 for Government 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.

Common Luna Architecture

All Luna HSMs benefit from a Common Luna Architecture where the supported client, APIs, algorithms, and authentication methods are consistent across the entire Luna 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.

Cryptographic Capabilities

Luna G5 for Government 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 for Government also supports ECC key pairs for use in Suite B applications that require a permanent, factory generated digital ID.

Security Certification

The Luna G5 for Government has received FIPS 140-2 Level 2 and 3 validation from the National Institution of Standards and Technology (NIST). This validation signifies that TCT's Luna HSMs for Government comply with these stringent standards.

Performance and Scalability

Luna G5 for Government
• RSA-1024 200 tps • RSA-2048 63 tps • ECC P256 43 tps • AES-GCM 71tps

Benefits

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

Technical Specifications

Operating System

- Windows, Linux

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

Physical Characteristics

- Dimensions: 8.5" x 6.7" x 1.7"
- Weight: 3.3lb (1.5kg)
- Power Consumption: 12W maximum, 8W typical
- Temperature: operating 0°C – 50°C

Security Certifications

- FIPS 140-2 Level 2 and Level 3 Validation

Safety and Environmental Compliance

- UL, CSA, CE
- FCC, KC Mark, VCCI, CE
- RoHS, WEEE

Host Interface

- USB 2.0

Reliability

- Mean Time Between Failure (MTBF) 858,824 hours

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., protects the most vital data from the core to the cloud to the field. We serve as a trusted, U.S. based source for cyber security solutions for the U.S. Federal Government. Our solutions enable agencies to deploy a holistic data protection ecosystem where data and cryptographic keys are secured and managed, and access and distribution are controlled.

Contact Us: For more information, visit www.thalestct.com