Thales Luna USB HSM

Versions 5.x and 6.x

The Thales Luna USB Hardware Security Module (HSM) is a small form factor HSM. Governments, financial institutions, and large enterprises reduce security risks and ensure regulatory compliance with this hardware cryptographic root of trust for data, applications and digital identities. It is well suited for the strong protection of Certificate Authority (CA) root keys and proof of concepts (PoCs).

Thales Luna USB HSM Overview

Thales Luna USB HSM delivers industry-leading key protection, exclusively maintaining all key materials 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 CA root keys.

Cryptographic Capabilities

Luna 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 Luna USB HSM has a hardware-implemented random number generator, compliant with NIST SP 800-90.

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

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

Benefits & Features

Most Secure

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

Sample Applications

- PKI key generation and key storage (online and offline CA keys)
- Certificate validation and signing

Tamper Recovery Role

The Luna 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 Luna 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 Luna 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

The Thales 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 Thales Luna 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
- TAA

Host Interface

- USB 2.0

Reliability

- MTBF: 858,824 hours

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

> thalesgroup.com <

Americas – Arboretum Plaza II, 9442 Capital of Texas Highway North, Suite 100, Austin, TX 78759 USA • Tel: +1 888 343 5773 or +1 512 257 3900 • Fax:+1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel:+852 2815 8633 • Fax:+852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – 350 Longwater Ave, Green Park, Reading, Berkshire, UK RG2 6GF • Tel:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com