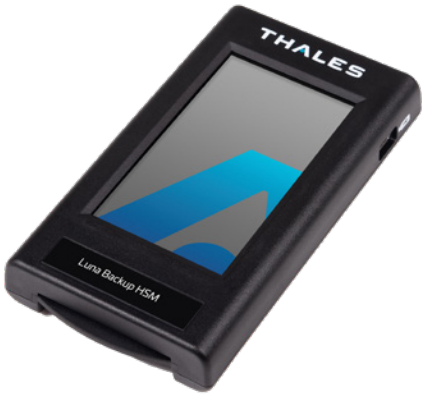
cpl.thalesgroup.com

THALES
Building a future we can all trust

Luna Backup HSM

Luna Backup Hardware Security Modules (HSMs) are widely used by enterprises, financial institutions and governments to securely backup high value cryptographic key material. This accessory to Luna Network and PCIe HSMs enables you to reduce risks, maintain SLAs, and ensure regulatory compliance, ensuring your critical data is securely stored offline.

They constitute a key element of your crypto agility strategy with their comprehensive support of symmetric and asymmetric key types and lengths.



Features & Benefits

Highest Security & Compliance:

- Keys always remain in FIPS validated*, intrusion-resistant, tamper-evident hardware
- Remote management, backup and restoration for quick disaster recovery
- LCD touch screen enables quick review of status including firmware, memory capacity, and more
- Standalone support of Quorum (MofN) multi-factor authentication for increased security

* in progress

Secure backup

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 cryptographic systems.

The Luna Backup HSM ensures your sensitive cryptographic material remains strongly protected in the hardware even when not being used. You can easily backup and duplicate keys securely to the Luna Backup HSM for safekeeping in case of emergency, failure or disaster. The remote backup capabilities allow administrators to securely replicate sensitive cryptographic key material to other Luna HSMs. With a single Luna Backup HSM, an administrator can backup and restore keys to and from up to 100 partitions.

The Luna Backup HSM provides the same level of security as the Luna Network and PCIe HSMs in a convenient, small and low cost form factor.

High assurance key protection

By its very name, HSM implies hardware. As such, most security professionals assume that all HSMs actually store cryptographic keys in hardware, as Luna HSMs do by default. In fact, while other leading HSMs generate their keys in hardware, they actually store the cryptographically wrapped keys on an application server. These keys, residing in software, can be easily detected—creating an additional attack surface.

The advantages of hardware are the key reasons why the world's largest enterprises and government organizations trust Luna HSMs to guard more digital identities and interbank fund transfers than any other HSM in the world.

Built for ease of use

- Easy setup – up and running in minutes
- Portable, handheld, small form factor device
- LCD touch screen enables quick review of status including firmware, memory capacity, and more
- Token authentication with dedicated USB port
- Host powered USB – no need for a power adaptor

Technical specifications

- **HSM B700,** 100 partitions, 32MB of storage space
- **HSM B750,** 100 partitions, 128MB of storage space
- **HSM B790,** 100 partitions, 256MB of storage space

Operating System Support

- Windows, Linux

Client

- Thales Luna Universal Client Security Certifications

Security Certification

- FIPS 140-3 Level 3*

Physical Characteristics

- Dimensions: 6.3" x 3.43" x 1.03" (160.02mm x 87.12mm x 26.16mm)
- Weight: 0.9lb (410g)
- 4.7" LCD touch screen
- Temperature: operating 0°C – 40°C, storage -20°C – 70°C
- Relative Humidity: 20% to 95% (38°C) non-condensing
- Power Consumption: 7.2W maximum, 4.5W typical
- External USB AC: Input Voltage: 100 - 240V, 50 - 60Hz / Output 5VDC 3A
- Host interface: USB 3.0 Type C connector
- Token interface: USB 3.0 Type C connector + USB-C (M) to USB-A (F) adapter

Safety and Environmental Compliance

- UL, CSA, CE
- FCC, KC Mark, VCCI, CE
- RoHS, WEEE
- India BIS [IS 13252 (Part 1)/IEC 60950-1]*

Reliability

- MTBF: 560073 hrs@40C, Telcordia SR-332, Issue C

Trade Agreement Compliance

- TAA

*in progress