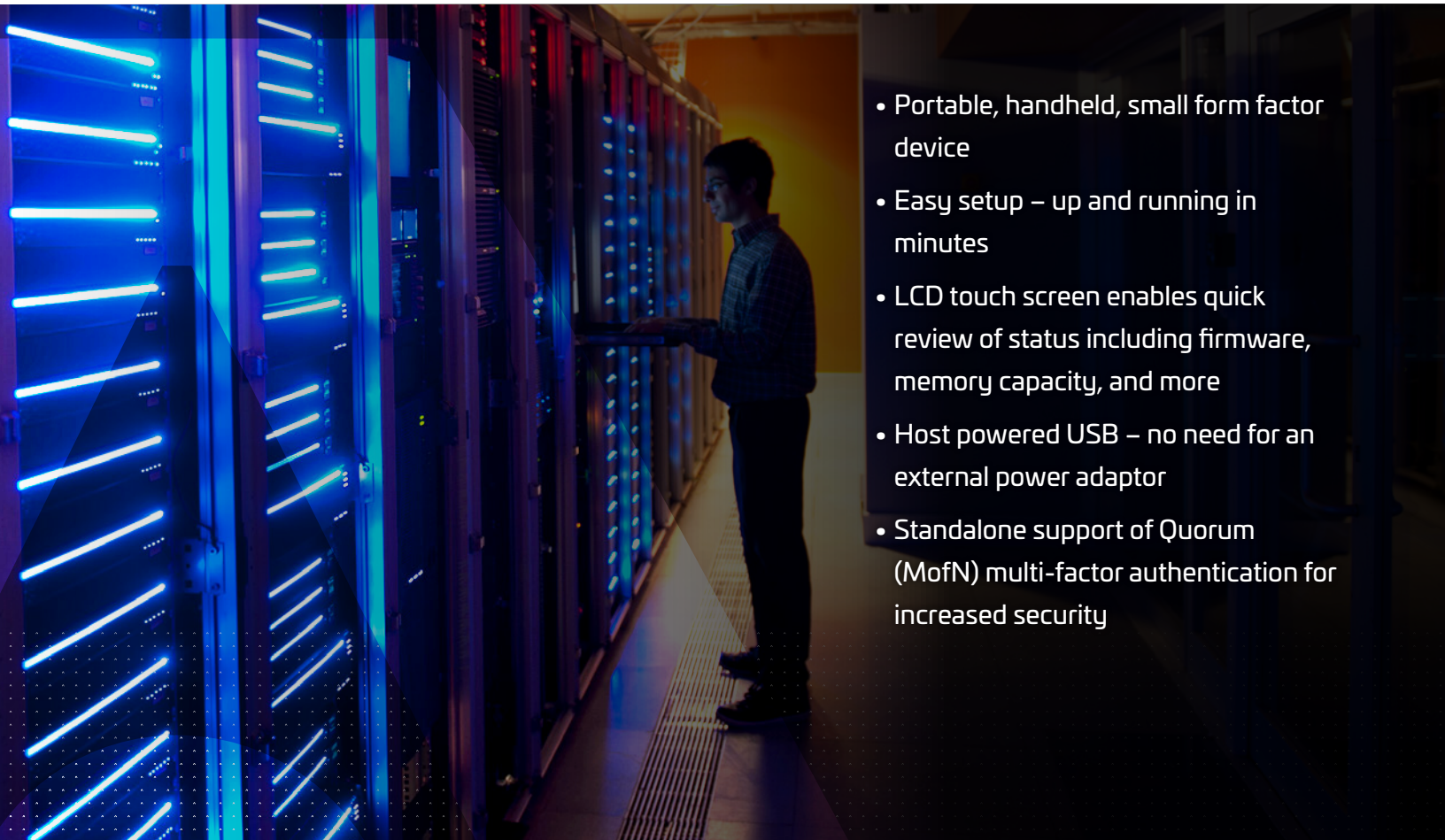
cpl.thalesgroup.com

THALES
Building a future we can all trust

Luna USB HSM

The Luna USB HSM is a small form factor HSM that is widely used by governments, financial institutions and large enterprises to protect data, applications and digital identities in order to reduce risk and ensure regulatory compliance. It is well suited for the strong protection of PKI root keys.



- Portable, handheld, small form factor device
- Easy setup – up and running in minutes
- LCD touch screen enables quick review of status including firmware, memory capacity, and more
- Host powered USB – no need for an external power adaptor
- Standalone support of Quorum (MofN) multi-factor authentication for increased security

Luna USB HSM Overview

The Luna USB HSM delivers high assurance key protection, maintaining all key materials encrypted within the confines of the tamper-resistant hardware. The small form factor and offline key storage capability set the product apart, making it ideal for protecting business critical keys in a secure offline environment.

Common Architecture

Luna HSMs benefit from a common architecture across the entire product line including Luna Network, Luna PCIe and Luna Cloud HSM where the client, APIs, algorithms, and authentication methods are consistent. This eliminates the need to design applications around a specific HSM, and provides the flexibility to clone keys from HSM to HSM and from on-premises to public and private clouds as your business needs change.

Benefits & Features

High Assurance Security

- Keys always remain in FIPS 140-3 validated*, intrusion-resistant hardware
- Remote management, backup and restore for quick disaster recovery
- Password Authentication or Quorum (MofN) multi-factor authentication for increased security and strong separation of duties
- High-assurance delivery with secure transport mode

Sample Applications

- PKI key generation and key storage/protection (online and offline CA keys)
- Certificate validation and signing
- Offline hardware protection/security of business critical keys
- Support Bring your own Key (BYOK) use cases

Crypto Agility

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 based random number generator, compliant with NIST SP 800-90A and B.

Performance

Operation	Key	TPS
Sign	RSA-1024	340
Sign	RSA-2048	62
Sign	RSA-4096	8
Sign	ECC P256	48
Sign	ECC P521	8
Encrypt	ECIES (AES128-SHA256 HMAC P256)	24
Encrypt	AES256-GCM	1350

Technical Specifications

Luna USB HSM U700

- 1 partition, 32MB

Operating System Support

- Windows, Linux

Client

- Thales Luna Universal Client

Cryptographic API Support

- PKCS#11, Java (JCA/JCE), Microsoft CAPI and CNG, OpenSSL

Cryptography

- Full Suite B support
- Asymmetric: RSA, DSA, Diffie-Hellman, Elliptic Curve Cryptography (ECDSA, ECDH, Ed25519, ECIES), KCDSA, and more
- Symmetric: AES, AES-GCM, Triple DES, DES, ARIA, SEED, RCS, RC4, RC5, CAST, and more
- Hash/Message Digest/HMAC: SHA-1, SHA-2, SHA-3, SM2,SM3, SM4 and more
- Key Derivation: SP800-108 Counter Mode
- Key Wrapping: SP800-38F
- RNG: Uses an hardware entropy source alongside a NIST 800-90A and B Hash-DRBG
- Digital Wallet Encryption: BIP32

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