cpl.thalesgroup.com

THALES
Building a future we can all trust

Thales 5G Luna Network HSM

Secure your critical 5G networks and easily scale with Thales 5G Luna Network Hardware Security Modules (HSMs). The 5G Luna HSM offers high assurance key protection, and up to 6,070 transactions per second (tps) for Profile B Decrypt P-256, 1,660 tps for Profile A Decrypt 25519, to meet security, throughput, and scalability requirements for 5G.

Protect subscriber sensitive data for 5G/4G with Luna HSMs:

- **Subscriber Privacy:**
  - Generate encryption keys, store home network private keys, and perform crypto operations to de-conceal the SUCI with the FIPS 140-2 Level 3 validated Luna HSM to protect the subscriber privacy.
- **Subscriber Authentication Vector Generation:**
  - Store master keys and run authentication algorithms within the secure confines of the Luna HSM to protect authentication-related keys during the authentication execution process.
- **Subscriber Key Provisioning:**
  - Store encryption keys for provisioning and storage systems, and perform encryption/decryption of provisioning and storage system keys, to secure authentication-related keys during SIM personalization and provisioning.
- **PKI Root of Trust:**
  - Secure your entire PKI-based telco infrastructure in a FIPS 140-2 Level 3 validated and Common Criteria EAL 4+ certified 5G Luna HSM hardware root of trust.

Contact us to learn how the tamper-resistant 5G Luna HSM is easily integrated to provide the protection you need for your entire critical 5G infrastructure.

What you need to know:

Superior Performance:

- Meet your high throughput and scalability requirements with a single HSM offering over 1,660 ECIES Profile A Decrypt 25519 tps, and 6,070 tps for Profile B Decrypt P-256
- Clustering offering up to 3,440 tps for Profile A and 12,000 tps for Profile B
- Lower latency for improved efficiency

Highest Security & Compliance:

- 5G encryption keys always remain in FIPS-validated, tamper-evident hardware
- 5G Cryptographic Mechanisms for Subscriber Authentication support: Milenage, Tuak, and COMP128
- Quantum resistance and high quality keys through crypto agility and external Quantum RNG seeding
- Meet compliance for data privacy regulations including GDPR
- De facto standard for the cloud
- Multiple roles for strong separation of duties
- Multi-person MofN with multi-factor authentication for increased security
- Secure audit logging
- High-assurance delivery with secure transport mode
- Securely backup and duplicate keys in hardware

Reduce Costs & Save time:

- Remotely manage HSMs - no need to travel
- Reduced audit and compliance costs and burdens
- Automate enterprise systems to manage HSMs via REST API
- Efficiently administer resources by sharing HSMs amongst multiple applications or tenants
- Flexible partition policies to meet your key management and compliance needs
- Increased portability, greater efficiency and less overhead using Luna Client in a container
- Functionality Modules
  - Extend native HSM functionality
  - Develop and deploy custom code within the secure confines of the HSM, for example proprietary subscriber authentication mechanisms

	Single 5G Luna HSM				High Availability Cluster 2 5G Luna HSMs			
Number of threads	1	10	20	50	1	10	20	50
ECIES Profile B Decrypt P-256	1,080 TPS	5,730 TPS	5,910 TPS	6,070 TPS	1,060 TPS	9,000 TPS	11,500 TPS	12,000 TPS
ECIES Profile B Decrypt P-256 (including key decompression)	700 TPS	2,000 TPS	2,000 TPS	2,000 TPS	730 TPS	3,770 TPS	4,040 TPS	4,190 TPS
ECIES Profile A Decrypt 25519	350 TPS	1,600 TPS	1,670 TPS	1,660 TPS	350 TPS	1,250 TPS	3,160 TPS	3,440 TPS

Technical specifications

Supported 5G Operating Systems

- Windows, Linux, Solaris, AIX
- Virtual: VMware, Hyper-V, Xen, KVM, API Support
- PKCS#11, Java (JCA/JCE), Microsoft CAPI and CNG, OpenSSL
- REST API for administration

Cryptography

5G Specific Algorithms

- 5G Cryptographic Mechanisms for Subscriber Authentication: Milenage, Tuak, and COMP128
- 5G Cryptographic Mechanisms for Subscriber Privacy: ECIES Profile A Decrypt 25519 and ECIES Profile B Decrypt P-256

Other

- Full Suite B support
- Asymmetric: RSA, DSA, Diffie-Hellman, Elliptic Curve, Cryptography (ECDSA, ECDH, Ed25519, ECIES) with named, user-defined and Brainpool curves, KCDSA, and more
- Symmetric: AES, AES-GCM, Triple DES, DES, ARIA, SEED, RC2, 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
- Random Number Generation: designed to comply with AIS 20/31 to DRG.4 using HW based true noise source alongside NIST 800-90A compliant CTR-DRBG
- Digital Wallet Encryption: BIP32

Security Certifications

- FIPS 140-2 Level 3 – Password and Multi-Factor (PED)
- Common Criteria EAL4+ (AVA_VAN.5 and ALC_FLR.2) against the Protection Profile EN 419 221-5
- Qualified Signature or Seal Creation Device (QSCD) listing for eIDAS compliance
- Singapore NITES Common Criteria Scheme

Host Interface

- 2 options: 4 Gigabit Ethernet ports with Port Bonding, or 2 x 10G fiber network connectivity and 2 x 1G with Port Bonding
- IPv4 and IPv6

Physical Characteristics

- Standard 1U 19in. rack mount appliance
- Dimensions: 19" x 21" x 1.725" (482.6mm x 533.4mm x 43.815mm)
- Weight: 28lb (12.7kg)
- Input Voltage: 100-240V, 50-60Hz
- Power Consumption: 100W maximum, 84W typical
- Heat Dissipation: 376BTU/hr maximum, 287BTU/hr typical
- Temperature: operating 0°C – 35°C, storage -20°C – 60°C
- Relative Humidity: 5% to 95% (38°C) non-condensing

Safety & Environmental Compliance

- UL, CSA, CE
- FCC, CE, VCCI, C-TICK, KC Mark
- TAA
- India BIS [IS 13252 (Part 1)/IEC 60950-1]

Reliability

- Dual hot-swap power supplies
- Field-serviceable components
- Mean Time Between Failure (MTBF) 171,308 hrs Management & Monitoring
- HA disaster recovery and performance scalability
- Backup and restore hardware to hardware on-premises or in the cloud
- SNMP, Syslog

Contact:

Chen Arbel
Vice President Business Development,
Global Head Of 5G & Cloud Security @ Thales
chen.arbel@thalesgroupo.com