Solution Brief

Thales Luna HSM for 5G Performance Measurements

cpl.thalesgroup.com

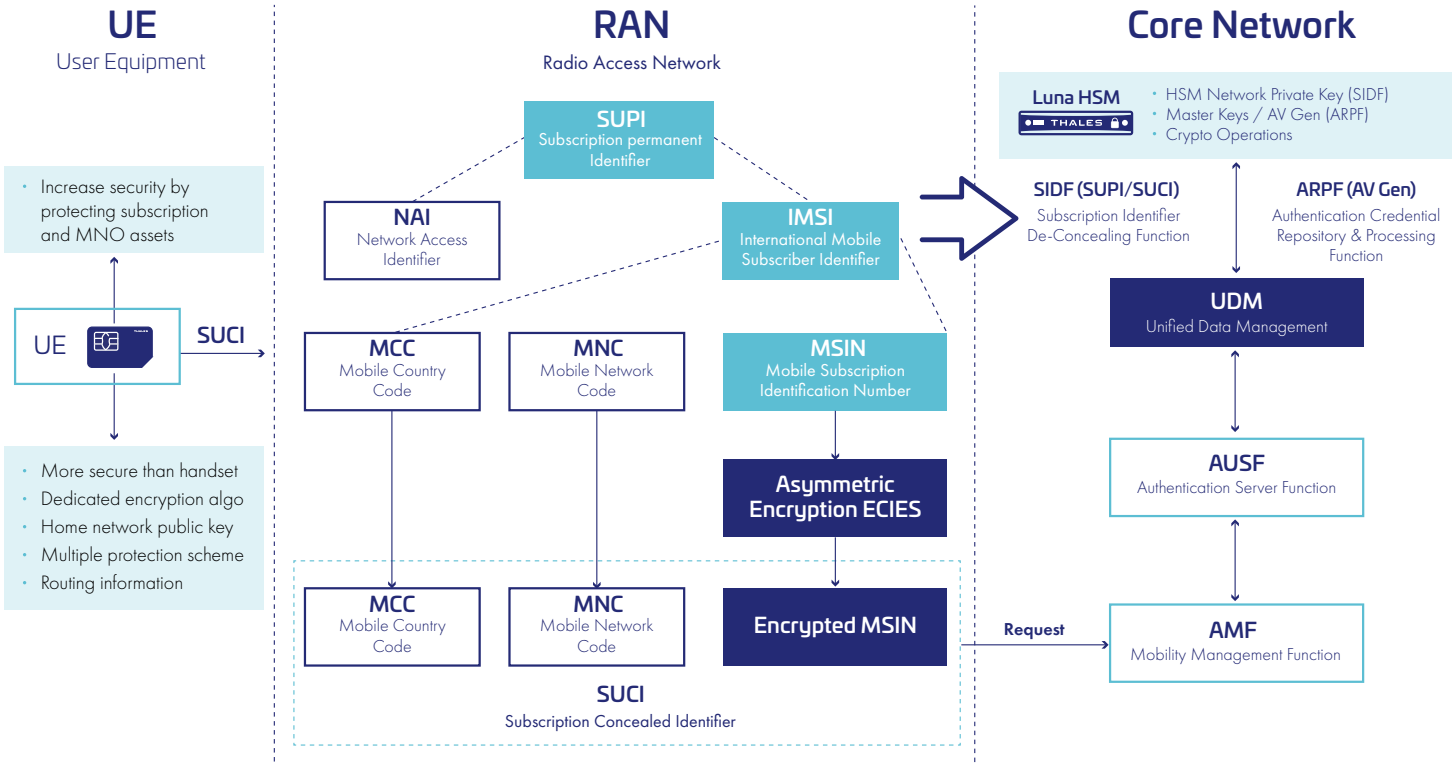
THALES
Building a future we can all trust

THALES
Building a future we can all trust

Thales 5G Luna Hardware Security Modules (HSMs) specifically address the throughput needs required by Network Equipment Providers (NEPs) and Mobile Network Operators (MNOs) for 5G.

Thales has optimized its **Luna Network HSMs** to meet the performance, flexibility, scalability, and high availability needed for 5G security:

- Meet the demanding high throughput and efficiency requirements for 5G
- Easily scale to satisfy service level agreements (support clustering with up to 32 members)
- Reduced total cost of ownership:
  - Up to 1,700 ECIES Profile A Decrypt 25519 tps, and up to 7,000 tps for Profile B Decrypt P-256
  - Up to 6.200 TPS Milenage or Comp Tuak Auth Vector Gen
  - Less hardware means less to set up, update and manage
- Low latency with fast response times
- Meet performance needs while maintaining a high assurance security posture



SUCI Decryption Performance Measurements

Number of HSM in HA group	1	2	8
ECIES P-256 Decrypt (decompressed keys)	7,000 TPS	14,000 TPS	56,000 TPS
ECIES P-256 Decrypt (compressed keys)	2,000 TPS	4,000 TPS	16,000 TPS
ECIES 25519 Decrypt	1,700 TPS	3,400 TPS	13,600 TPS

Subscriber Authentication Vector Generation Performance

Number of HSM in HA group	1	2	8	Parameters format
Milenage **(performance varies depending on the parameters format)**	4,200 TPS 6,200 TPS	8,400 TPS 12,400 TPS	33,600 TPS 49,600 TPS	eOPc and RC values OP handle and a RC value
Comp Tuak **(performance varies depending on the parameters format)**	4,300 TPS 6,300 TPS	8,600 TPS 12,400 TPS	34,400 TPS 50,400 TPS	eOP value OP handle

Test system configuration

- Test System
  - Mem: 16GB, Processor: Intel® Xeon(R) CPU E5-2640 v4 @ 2.40GHz × 40 (40 cores), 64 bit CentOS8
  - Luna network HSM A790 – local network with very low latency
- Multi threads and high availability for optimal performance
  - Maximum performance is obtained using multi threads and by configuring high availability clusters

Performance depends on the paramater format: The authentication generation function supports different parameter formats and encryption modes that may affect the performance. We indicate both the lowest performance configuration and the highest performance configuration.

Ki / OP key block protection

- The encryption/decryption mechanism used to protect the Ki and OP is the NIST approved CKM_AES_KWP (PKCS # 11 definition) and where the default IV (per NIST SP800-38F) is used.