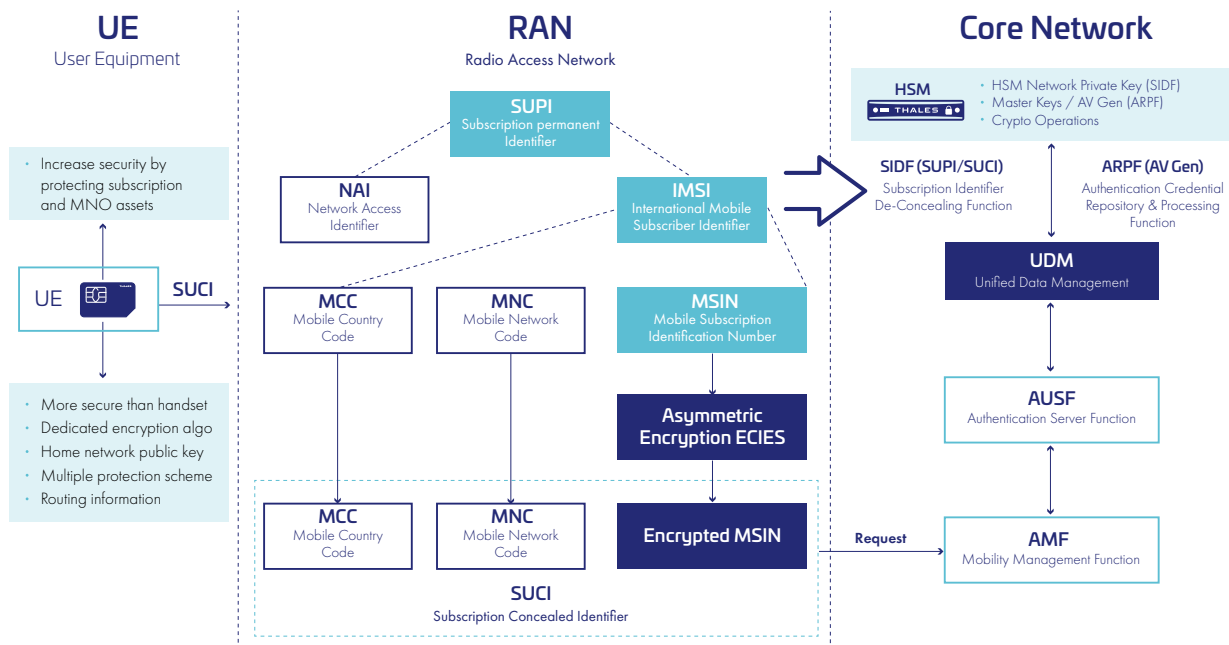


# Thales Luna HSM for 5G Performance Measurements

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.

**Offering up to three times the performance offered by competitive solutions, NEPs and MNOs can now:**

- Meet the demanding high throughput and efficiency requirements for 5G
- Easily scale to satisfy service level agreements
- Reduced total cost of ownership:
  - One Luna HSM offering 1,660 tps for Profile A Decrypt 25519
  - 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



## ECIES Profile A and Profile B Decryption Performance Measurements

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

## Thales 5G Luna HSM Authentication Vector Gen Performance

	Single HSM				HA Cluster 2 HSM			
	1	10	20	50	1	10	20	50
<b>Number of threads</b>	1	10	20	50	1	10	20	50
<b>3GPP Milenage</b>	2,538 TPS	4,770 TPS	4,786 TPS	4,629 TPS	2,415 TPS	9,371 TPS	9,468 TPS	9,531 TPS
<b>3GPP TUAK</b>	3,106 TPS	6,020 TPS	6,026 TPS	5,930 TPS	2,584 TPS	11,695 TPS	11,833 TPS	11,837 TPS

## Test system configuration





- Test System
  - Mem: 16GB, Processor: Intel® Xeon(R) CPU E5-2640 v4 @ 2.40GHz × 40 (40 cores), 64 bit CentOS8
- Multi threads and high availability for optimal performance
  - Maximum performance is obtained using multi threads and by configuring high availability clusters
- Compressed key format – P-256
  - In the case of the P-256 curve, performance is provided with and without public key decompression (can be performed by the HSM or by the telecom operator platform)

## 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.

## Questions?

Contact Chen Arbel, VP Business Development, Head of 5G and Cloud Security, Cloud Protection and Licensing Division, [chen.arbel@thalesgroup.com](mailto:chen.arbel@thalesgroup.com), +1-845-300-5444 should you have any questions or need additional information.

> [cpl.thalesgroup.com](http://cpl.thalesgroup.com) <    

**Contact us** – For all office locations and contact information, please visit [cpl.thalesgroup.com/contact-us](http://cpl.thalesgroup.com/contact-us)