cpl.thalesgroup.com

THALES
Building a future we can all trust

5G Subscriber Privacy and Authentication HSM Protection

The introduction of 5G presents Network Equipment Providers (NEPs) and Mobile Network Operators (MNOs) with the need to provide wider bandwidth, higher capacity, multi-Gbps throughput, more reliability and lower latency. Furthermore, the complexity of the infrastructure; the distributed nature of the 5G networks; the astounding number of devices including the growth in the Internet of Things (IoT) add to this complexity. And if that isn't enough, the use of open source platforms and multi-vendor networks; cloud; and the evolution from 3G and 4G networks all present challenges to ensuring the protection and authenticity of subscriber authentication and privacy.

To help NEPs and MNOs address security challenges, Thales has optimized its Luna Network Hardware Security Module (HSM) for 5G use cases. Offering up to 6,070 transactions per second (tps) for Profile B Decrypt P-256, 1,660 tps for Profile A Decrypt 25519 with a single HSM, and a PKI hardware-based root of trust, the 5G Luna Network HSM meets the high availability and scalability needs from the data center to the edge. Furthermore, performing all crypto operations and storing, generating and managing encryption keys within the secure confines of the 5G Luna HSM ensures subscriber identities including the Subscription Concealed Identifier (SUPI), user equipment, radio area networks (RANs), and their core network infrastructure are well protected.

5G RAN and core networks rely heavily on authentication, authorization, and encryption. Verifying the identity of the subscriber and encrypting communications relies on trusting the private keys being used. In 5G networks, HSMs act as trust anchors that protect the cryptographic infrastructure used to establish identities across the network. The 5G Luna HSM enhances subscriber privacy and authentication by offering a secure mechanism for the Subscription Identifier De-concealing Function (SIDF), Authentication Credential Repository and Processing Function (ARPF), Authentication Server Function (AUSF), Unified Data Manager (UDM), and Unified Data Repository (UDR) to ensure that the encryption keys are always protected.

What is an HSM?

An HSM is a dedicated device specifically designed for the protection of the cryptographic keys. HSMs act as trust anchors that protect the cryptographic infrastructure of some of the most security-conscious organizations in the world by securely managing, processing, and storing those keys inside a purpose made device.

The need for a strong crypto foundation

A root of trust is the foundation of a cryptographic system. Digital security is dependent on cryptographic keys that encrypt and decrypt data and perform functions such as signing and verifying signatures and ensuring the integrity of those keys and the cryptographic functions within a secure environment such as an HSM is paramount.

A strong foundation of trust for your 5G infrastructure means all devices, data, transactions, and users are well protected. Meet the high demands of industry regulations and audit requirements in addition to achieving your business and revenue goals, without compromising agility, usability or scalability.

Thales 5G Luna HSM

Luna HSMs have been protecting businesses and people for decades, and evolving over the years to meet the challenges of new technologies such as 5G. The 5G Luna HSM, a tamper-resistant, network-attached appliance, stores, protects and manages cryptographic keys in a hardware root of trust. Securing 5G data, transactions, users and devices within the hardware root of trust ensures high assurance protection of the master storage key that encrypts all identities issued to devices; strong entropy; and strict authentication controls.

5G Luna HSM Benefits

- We're fast! Up to 1,660 tps for Profile A 22519 and 6,070 for Profile B P-256
- Support 5G Cryptographic Mechanisms for Subscriber Authentication: Milenage, Tuak, and COMP128
- Keys in hardware approach – all crypto performed within the secure confines of the HSM
- Hardware root of trust ensures security from the infrastructure layer to the application layer
- Leader in the PKI protection space, future-proofing deployments with post-quantum crypto agility
- HSM code/container signing and validation

5G HSM Use Cases

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.
  - Protect your 5G cloud infrastructure - Connect your Luna HSM to the Thales CipherTrust Manager to secure your 5G cloud infrastructure (databases, file servers, TLS/SSL keys, virtual machines).

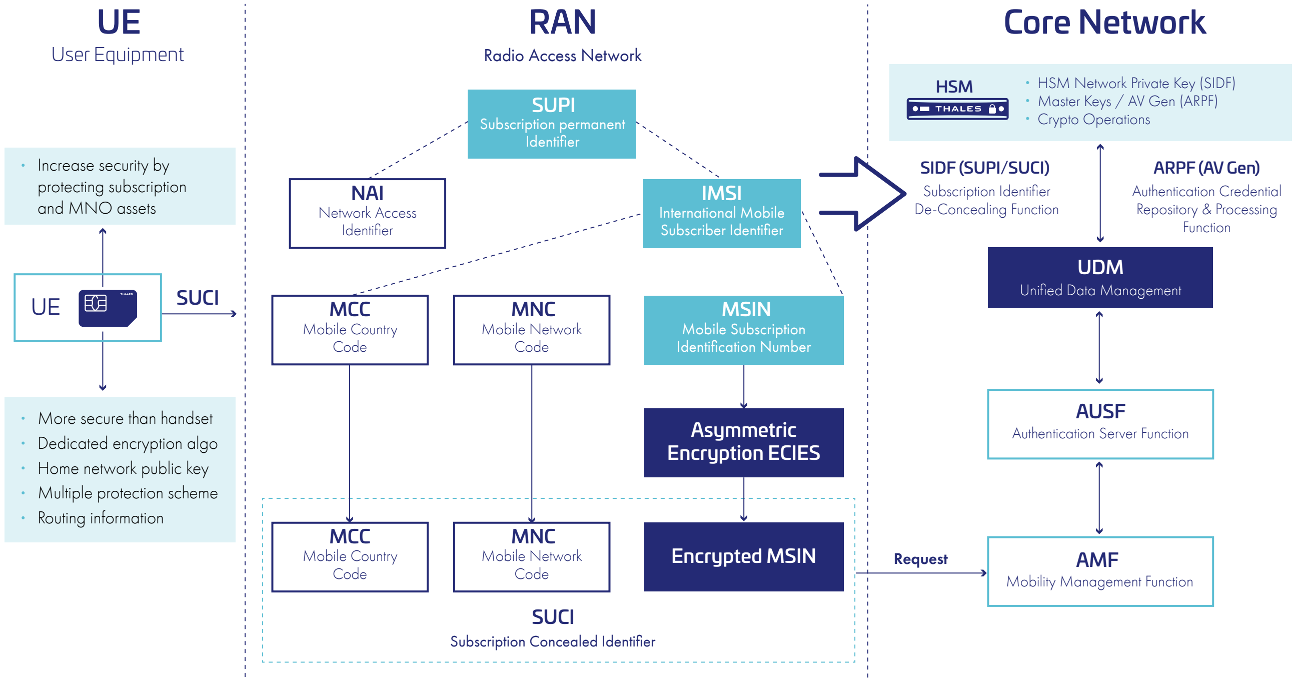
UE
User Equipment
Increase security by protecting subscription and MNO assets
UE
SUCI
More secure than handset
Dedicated encryption algo
Home network public key
Multiple protection scheme
Routing information
RAN
Radio Access Network
SUPI
Subscription permanent Identifier
NAI
Network Access Identifier
IMSI
International Mobile Subscriber Identifier
MCC
Mobile Country Code
MNC
Mobile Network Code
MSIN
Mobile Subscription Identification Number
Asymmetric Encryption ECIES
MCC
Mobile Country Code
MNC
Mobile Network Code
Encrypted MSIN
SUCI
Subscription Concealed Identifier
Core Network
HSM
THALES
HSM Network Private Key (SIDF)
Master Keys / AV Gen (ARPF)
Crypto Operations
SIDF (SUPI/SUCI)
Subscription Identifier De-Concealing Function
ARPF (AV Gen)
Authentication Credential Repository & Processing Function
UDM
Unified Data Management
AUSF
Authentication Server Function
Request
AMF
Mobility Management Function

Diagram 1: 5G Core – Subscriber Privacy and AV Generation

Why the Need for HSM Performance?

The performance offered by the 5G Luna HSM offers NEPs and MNOs the following advantages:

- 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 can do the job of 3+ competitive HSMs
    - 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

Keys in hardware approach

Ensure your critical encryption keys and digital identities are always secure and always know their whereabouts by generating, managing, and storing them in a hardware root of trust by default.

Crypto agility

Quickly react to threats by implementing crypto agile, alternative means of encryption. Future proof your organization by implementing quantum safe algorithms, securing your organization's users and data today and into the future.

Custom development

Develop and deploy custom code within the secure confines of the HSM with Functionality Modules (FMs). Implement you 5g/4g/3g proprietary or secret authentication algorithms, or provisioning algorithms in your own FM.

Always know the whereabouts of your keys

Securely isolate your cryptographic keys inside the tamper-resistant hardware of the 5G Luna HSM with our unique keys-in-hardware approach. Knowing cryptography is only as strong as the security afforded to your cryptographic keys, 5G Luna HSMs are designed with the highest key security in mind. Applications communicate with the keys stored in the Luna HSM via a client – but keys never leave the HSM.

Meet your compliance needs

Whatever your compliance needs may be, from GDPR and eIDAS to PCI-DSS and CCPA, 5G Luna HSMs are part of the solution. Luna HSMs offer the most certifications in the industry including Common Criteria, FIPS 140-2, ITI and more. Have complete trust in your 5G infrastructure, backed by a certified HSM cryptographic foundation that is internationally recognized.

Easily manage and monitor HSM resources

Manage your cryptographic resources with Thales Crypto Command Center, a centralized platform that provides on-demand monitoring, reporting, provisioning and alerting in minutes.

Extend your return on investment

Integrate with over 400 of the most commonly used enterprise applications - the largest ecosystem of partners in the market. Implement your Luna HSM as a root of trust with your favorite third party security solutions to protect your 5G cloud infrastructure (secrets database, customer databases, VM, SSL/TLS, code, and more). Additionally, benefit from a broad API support including PKCS #11, Java, Open SSL, Microsoft, Ruby, Python and Go.

Install and connect in modern data centers

Benefit from IPV6, optional 10G fiber/copper connectivity, low power requirements, and reduced TCO with remote management.

Thales can help

Address 5G security network vulnerabilities from the edge to the RAN and core with Luna Network HSMs.

Contact us to learn how to quickly adapt your infrastructure to meet the 5G performance, scalability, speed, cost and privacy requirements, and establish a root of trust for your critical infrastructure.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

> cpl.thalesgroup.com <

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us