Solution Brief

Thales CPL 5G Security Solutions from the Edge to the Core

Establishing integrity, confidentiality, and availability across 5G networks

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

5G connectivity is ready to transform industries and the way telcos operate, and 5G users will benefit from more connections with fewer drops and less interference, while enjoying remote access from almost anywhere. Though 5G creates extraordinary opportunities for people and businesses, this groundbreaking technology relies on virtualized, cloud-based, and multi-vendor architecture, which introduces unique technical and security challenges.

Network Equipment Providers (NEPs) and Mobile Network Operators (MNOs) need to provide wider bandwidth, higher capacity, multi-Gbps throughput, more reliability and lower latency. The distributed nature of 5G networks, the growing number of connected devices (IoT), the use of open-source platforms and multi-vendor networks, cloud adoption and increased entry points for cyber-attacks, add to the list of security challenges to address.

The Challenges

According to the '2023 Thales Data Threat Report Telecommunications Edition', telco companies, global enterprises and governments share the same areas of concern when it comes to addressing 5G cybersecurity:

Data in Motion: Securing data moving across 5G networks.

Identities: Protecting the identities of people and devices connecting to 5G networks.

Applications and Infrastructure: Securing applications, infrastructure, and sensitive data on 5G networks.

Thales provides 5G security solutions that help address these complex challenges and mitigate the threat to data integrity, availability, and confidentiality across 5G networks.

Thales CPL 5G Security Solutions

With 5G, different types of data will be processed at locations from the edge to the network core. Thales 5G security solutions deliver end-to-end encryption and authentication to protect data across fronthaul, midhaul, and backhaul operations as data moves from users and IoT, to radio access, to the edge (including multi-user edge computing) and finally, in the core network and data stores, including containers.

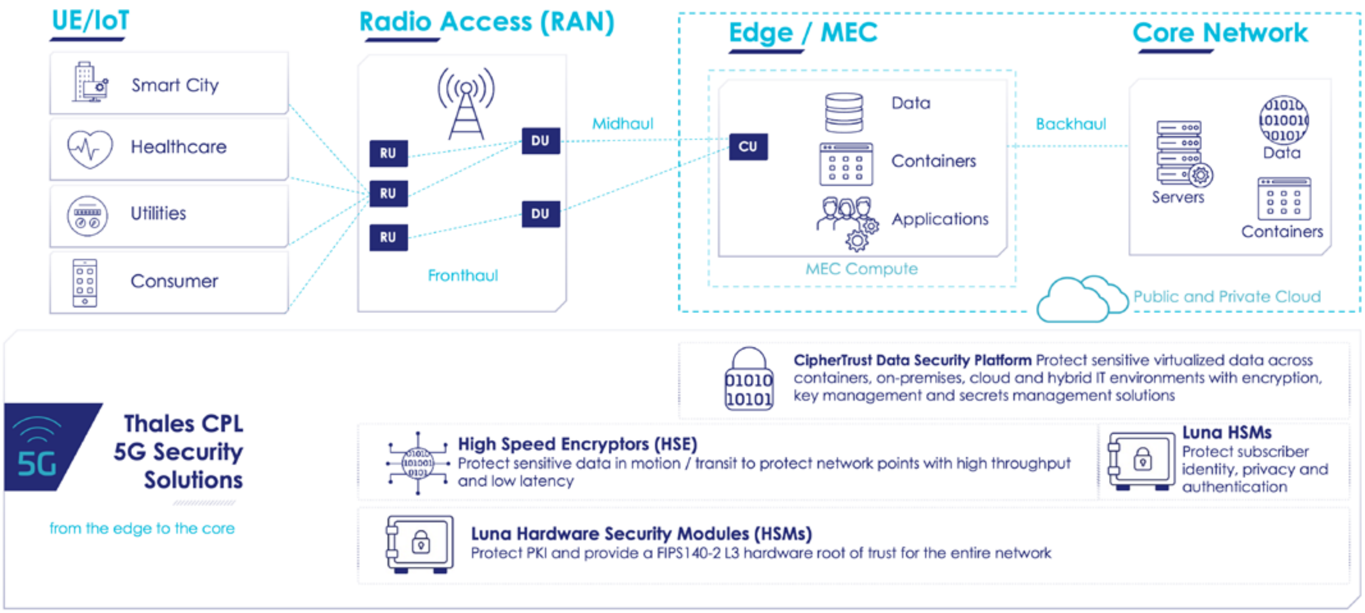
Protect Data in Motion with High Speed Encryption

Secure data in motion by encrypting all control plane traffic in the core, MEC and RAN with Thales High Speed Encryptors (HSE) solutions that provide:

Increased Performance: 5G promises remarkable speeds and larger data transfer potential, with substantially less wait times. HSEs are built for modern networks like 5G that demand enhanced security capabilities for data-in-motion protection, such as ultra-low latency, improved performance, compatibility with 5G network architecture, and scalability.

Network Security: A multi-point solution, HSE hardware and virtual appliances support a wide range of RAN/O-RAN network requirements such as network slicing. Unlike legacy solutions, Thales network encryption solutions are equipped with Transport Independent Mode (TIM), which allows for concurrent encryption over network Layers 2, 3 and 4, eliminating transport constraints and providing for optimum performance at the highest standards of network security.

Compliance and Quantum Readiness: Thales HSEs are certified by NIST – FIPS 140-2 Level 3, and by ANSSI – Common Criteria EAL 4+, and have been vetted by the US Department of Defense Information Systems Agency and by NATO, among others. Thales network encryption solutions uphold security best practices such as authenticated end-to-end encryption, automated key generation and updates, and controlled access (separation of duties). Crypto-agile, Thales HSEs are quantum ready, and offer field upgradeable support for all four NIST PQC (Post Quantum Crypto) algorithm finalists, and more as they evolve.



CipherTrust Data Security Platform Protect sensitive virtualized data across containers, on-premises, cloud and hybrid IT environments with encryption, key management and secrets management solutions

High Speed Encryptors (HSE) Protect sensitive data in motion / transit to protect network points with high throughput and low latency

Luna HSMs Protect subscriber identity, privacy and authentication

Luna Hardware Security Modules (HSMs) Protect PKI and provide a FIPS140-2 L3 hardware root of trust for the entire network

Protect Critical PKI Infrastructure, Subscriber Identity and Privacy with a Hardware Root of Trust

Thales has optimized its Luna Network Hardware Security Modules (HSMs) to provide a solution that meets the performance, flexibility, scalability, and high availability needed to help address the following 5G security concerns:

Subscriber Identities: Generate encryption keys, store home network private keys, and perform crypto operations to de-conceal SUCI within the Luna HSM to ensure subscriber identities and privacy, including the SUPI, are protected with a hardware root of trust.

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.

Strong Foundation of Trust for PKI: Secure the entire PKI-based telco infrastructure, digital certificates, and signatures by storing and managing the private keys used in code signing applications in a FIPS 140-2 Level 3 validated Luna HSM. Luna HSMs can also be used as a root of trust for Thales CipherTrust Manager to secure 5G cloud infrastructure (databases, file servers, TLS/SSL keys, virtual machines and containers).

Compliance and Quantum Readiness: Luna HSMs provide a FIPS 140-2 Level 3 and Common Criteria EAL 4+ certified crypto agile solution, enabling quantum safe algorithms to secure users and data today and into the future.

Luna HSMs offer the most certifications in the industry, including Common Criteria, FIPS 140-2, ITI and more. Have complete trust in the 5G infrastructure, backed by a certified HSM cryptographic foundation that is internationally recognized.

Protect Sensitive Data-at-Rest Across Hybrid Environments with CipherTrust Data Security Platform:

Strong encryption, combined with key management provides consistent protection for sensitive data and secrets across containers, on-premises, cloud, or hybrid environments. Thales CipherTrust Manager provides a single pane of glass, combining tools such as key management, CipherTrust Transparent Encryption (CTE), CipherTrust Cloud Key Management (CCKM), and CipherTrust Secrets Management (CSM) to meet the complex needs of 5G security:

Encrypt Sensitive Data-at-Rest Across 5G Networks: CipherTrust Transparent Encryption provides consistent encryption of sensitive data across all 5G network configurations and virtual network functions with granular access control. This solution encrypts data generated from containerized applications without any change to application business logic. The solution can also be deployed in a Kubernetes infrastructure allowing a containerized application to interact with existing persistent storage, which transparently protects the data.

Centralized Key Management: CipherTrust Manager centralizes cryptographic key management across multiple cloud vendors and hardware storage providers.

Strong Access Controls and Auditability: Ensure strict access controls and the capability to audit all file operation/access events to protected data. Users can monitor usage via SIEMs to better understand who is accessing the information.

Ensure Data and Application Security through Centrally Managed Secrets:

Quickly deploy and scale the Secrets Management SaaS application from the CipherTrust Manager dashboard, to protect and automate access to secrets across tools and cloud workloads, including credentials, certificates, API keys, and tokens. Rapidly deploy multi-cloud applications and speed-up continuous integration and delivery processes across hybrid, multi-cloud, multi-tenants, on-premises, as well as human or machine access.

Thales is Here to Help

Thales can support organizations with their 5G security strategy, including integration, deployment, and meeting compliance needs.

About Thales

Today's businesses and governments depend on the cloud, data and software to deliver trusted digital services. That is why the most recognized brands and organizations around the world, rely on Thales to help them protect sensitive information and software wherever it is created, stored or accessed – from the cloud and data centers to devices and across networks. As the global leader in data security, identity & access management, and software licensing, our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, create more value from their software and deliver seamless digital experiences for millions of consumers every day.