Solution Brief

Thales CPL Security Solutions for Private 5G

Establishing integrity, confidentiality, and availability across private 5G networks

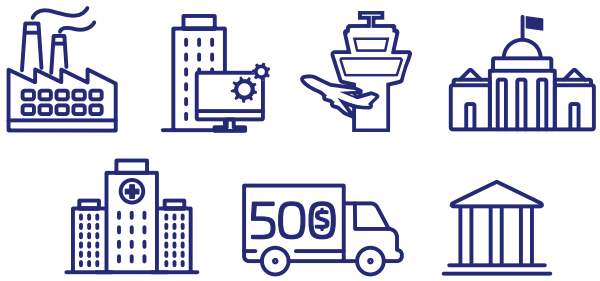
cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

Many businesses and organizations are seeking to leverage the transformative potential of 5G technology by implementing their own private 5G network, gaining unprecedented flexibility in how they address their unique connectivity requirements, enhanced privacy and security over sensitive data and communications, and the ability to adapt and expand their network capabilities as their business needs evolve.
These capabilities combined with performance factors like high reliability, scalability, speed, and lower latency are why these networks are being placed in mission critical infrastructures, and across highly regulated industries.

P5G Industries



Sample P5G Industries: healthcare, manufacturing / OT, transportation and logistics, utilities, agriculture and mining, defense and security, education.

The Challenges

Even though a private 5G network is inherently more secure than Wi-Fi and 4G, additional security is needed to protect sensitive data and critical infrastructure from unauthorized access, interception, and cyber-attacks. This is crucial for ensuring the integrity and confidentiality of network communications, as well as safeguarding against potential disruptions, unauthorized use of network resources and against any potential backdoor IT access for hackers. With the increasing adoption of Internet of Things (IoT) devices in industrial and enterprise settings, security is also essential for protecting interconnected systems and devices from potential vulnerabilities and cyber threats.

P5G Security Threats

Private 5G networks, like any other network, can face security vulnerabilities and threats and it's important to implement robust security measures due to the:

- Nature of sensitive data and mission critical applications being shared and stored
- Complexity of the network virtualization
- Larger attack surface
- Quantum threat (sensitive information transmitted over private 5G networks could be at risk if quantum-resistant encryption methods are not in place today)

The Solutions

Thales offers a range of solutions to bring enhanced security to private 5G networks:

Protect Operator and Authentication Keys, PKI, Subscriber Identity and Privacy with a Hardware Root of Trust

- Protect network keys, subscriber credentials and authentication algorithms
- Secure subscriber digital identities and privacy
- Hardware root of trust for your entire network, PKI and critical infrastructure

Meet the performance, flexibility, and scalability needed to secure subscriber privacy and authentication from the data center to the edge with Thales Luna Hardware Security Modules (HSMs). Luna HSMs have been a market leader for 25+ years and are available in various form factors including a hardened connected network appliance, USB-attached appliance, and a server-embedded PCIe card.

The Luna PCIe HSM is well suited for private 5G as it provides an easy-to-integrate and cost-efficient solution that can directly embed into an appliance or core application server for FIPS 140-3 Level 3 validated and Common Criteria EAL 4+ certified security. The high-security hardware design ensures the integrity and protection of encryption keys throughout their life cycle and all digital signing and verification operations are performed within the HSM to increase performance and maintain security.

Luna HSMs a certified, crypto agile foundation of digital trust, enabling quantum safe algorithms to secure users and data today and into the future.

Protect Data in Motion with High Speed Encryption

- When security, high bandwidth and low latency are required
- Secure data in motion from the RAN to the edge, from the edge to the core network guaranteeing the confidentiality and integrity of your data transmissions

Thales High Speed Encryption solutions (HSE) provide a multi-point solution and support a wide range of RAN/O-RAN private network requirements such as network slicing and are equipped with Transport Independent Mode (TIM), for concurrent encryption over network Layers 2, 3 and 4. Thales HSE hardware and virtual appliances are FIPS 140-2 Level 3 and Common Criteria EAL 4+ certified, are vetted

by the US Department of Defense Information Systems Agency and NATO. PQC ready and crypto agile, with support for all four NIST PQC algorithm finalists, and more as they evolve.

Protect Virtualized Data-at-Rest

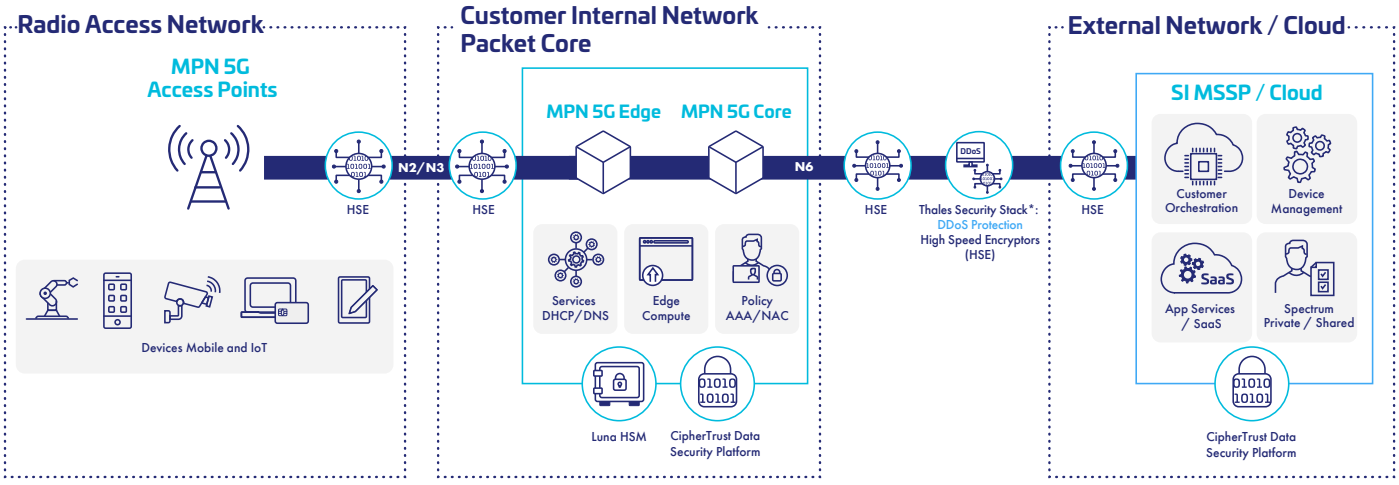
- Protect data-at-rest across public and private cloud environments
- Implement digital sovereignty controls
- Provide consistent encryption of sensitive data and secrets

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

Protect Against DDoS Attacks

- Secure your assets at the edge for uninterrupted operation
- Ensure business continunity with guaranteed uptime

The telecommunications industry has seen a dramatic surge in Distributed Denial of Service (DDoS) attacks, with a 548% increase in the first half of 2024 compared to the same period in the previous year. This alarming statistic, reported in Imperva's DDoS Threat Landscape Report, underscores the growing vulnerability of this sector. This sharp rise in attacks emphasizes the critical need for robust security measures, especially as 5G networks expand, further increasing the risk of disruption to vital communication services. Imperva DDoS Protection secures all your assets at the edge for uninterrupted operation to ensure business continuity with guaranteed uptime.



Thales CPL Solutions

Luna HSMs
Protect subscriber identity, privacy and authentication algorithms | PKI root of trust

CipherTrust Data Security Platform
Protect sensitive data across containers (Kubernetes) | Ensure data sovereignty

DDoS Protection
Secure your assets at the edge for uninterrupted operation

High Speed Encryptors (HSE)
Protect data in motion with high throughput and low latency

*Imperva DDoS & Thales HSE Integration testing underway

Thales is Here to Help

Thales can support organizations with their private 5G network security strategy, including integration, deployment, and addressing 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.

cpl.thalesgroup.com

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