cpl.thalesgroup.com

THALES
Building a future we can all trust

5G Data In Motion Security

The introduction of 5G networks within both physical and virtualized environments presents unparalleled challenges for securing data in motion. Legacy technologies, such as IPsec and MACsec, are unable to meet modern 5G demands for low latency, minimal jitter, and quantum-resistant, capacity-efficient data flows. From front haul to back haul, from decentralized user plane functions to any new interfaces, security and efficiency have never been more prominent requirements than within the 5G infrastructure. The security of separate and decentralized 5G interfaces require efficiency, timing, and unparalleled performance to meet end-user customer expectations.

Thales High Speed Encryptors (HSE) help network equipment providers (NEP) and mobile network operators (MNO) address these data in motion security challenges. With both hardware and virtualized network encryption solutions, the Thales HSE can encrypt 5G data flows from 10Mbps to 100Gbps within the radio access network (RAN) / open radio access network (O-RAN), core infrastructure, tower-to-tower, and cloud environments.

Virtual HSE for RAN / O-RAN and Integrated endpoints. Hardware HSE for up to 100 Gbps Backhaul and Core Infrastructures

> **" 5G transmits large amounts of data at high speeds that require low latency, near-zero jitter, and high throughput. Thales High Speed Encryptors (HSE) provide solutions for telco operators to overcome those obstacles by maximizing 5G security without compromising performance."**
>
> – Chen Arbel, VP Business Development,
> Head of 5G & Cloud Security

What is an HSE?

The Thales HSE is a data in motion security solution that provides network independent encryption. This capability is enabled by its Transport Independent Mode (TIM). By separating security from the transport layer, HSE combines the highest levels of data in motion security with the highest levels of transport efficiency, both of which are key requirements for 5G networks. Recent testing on a live 5G wired infrastructure shows that HSE reduces IPsec overhead by at least 25%. HSE also shows significant reductions in latency (measured in µSec) and the complete elimination of jitter (see Diagram 1), all of which are critical success factors within the 5G infrastructure. In addition to significantly increased performance, the Thales HSE is quantum ready, meaning all of the proposed standards-based, down-selected quantum algorithms are available today.

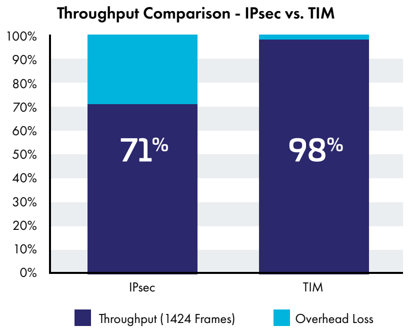


Figure 1 – IPsec vs. Thales Transport Independent Mode

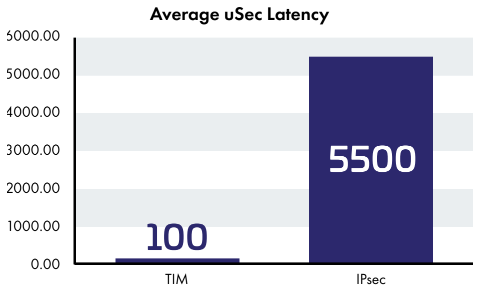


Figure 2 – IPsec vs. Thales TIM Latency over a 5G Infrastructure

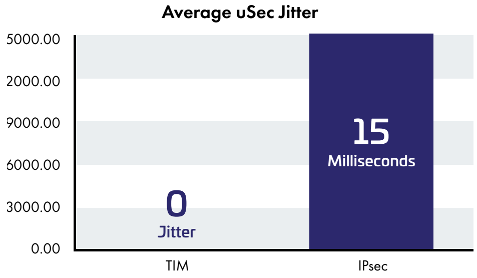


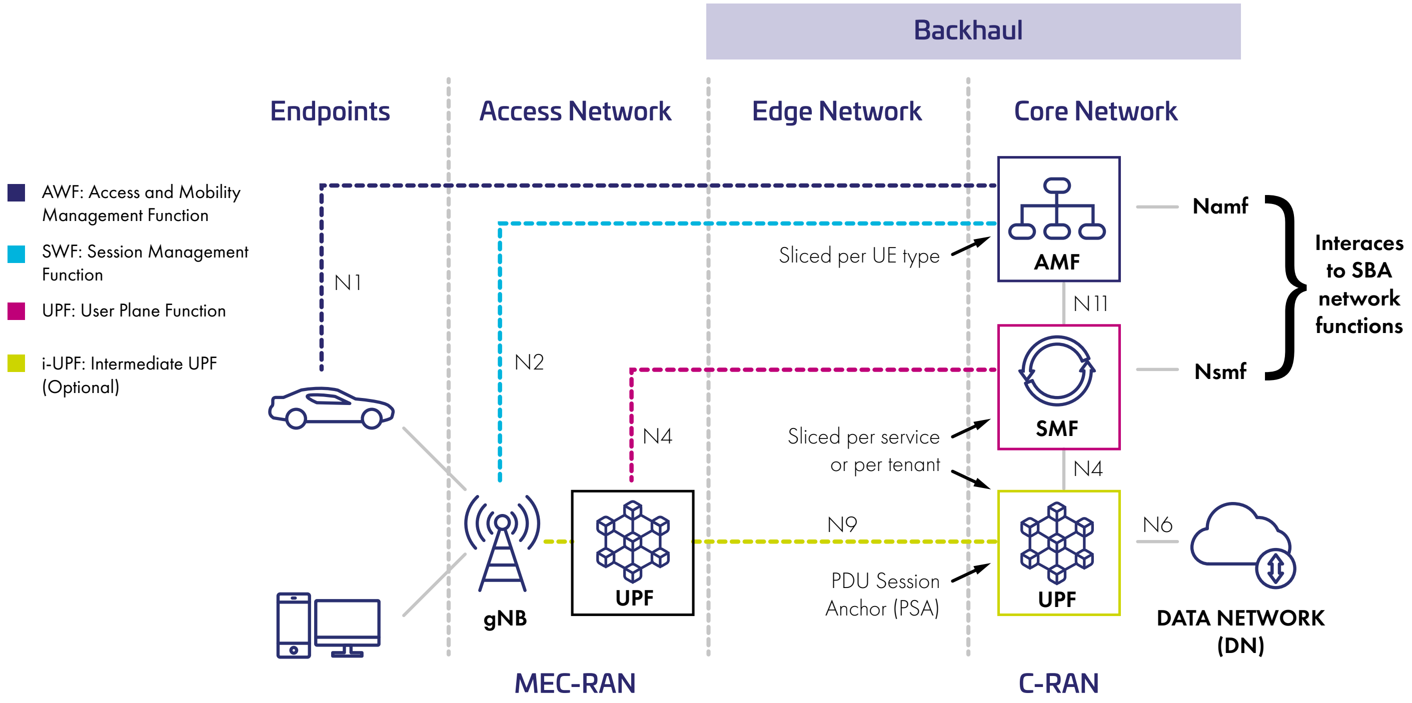
Figure 3 – IPsec vs. Thales TIM Jitter over a 5G Infrastructure

What Makes HSE so Efficient?

HSE is efficient because security functions have little to no interaction with the data flow protocol. As an example, IPsec adds at least 30% overhead to the transport layer. Additionally, IPsec encapsulates certain protocol enhancement techniques i.e. Performance Enhancing Proxy (PEP). Conversely, HSE only requires a small amount (~5%) of overhead and leaves the Layer 3 and Layer 4 transport protocols intact, and near-zero to zero overhead on Layer 2. This results in high levels of security and data integrity, with nearly zero impact on network performance. Even when protocol enhancement techniques are used, HSE provides unimpeded performance. Implemented as a simple bump-in-the-line security function, there is no need to redesign the network. Simply place the HSE network encryptors between the interfaces in which data flows are to be secured.

Thales HSE for 5G

Thales HSE's are available as both physical and virtual solutions,as a self-contained hardware endpoint, or it can be integrated into virtualized environments including white box and customized hardware. HSE can fit into any network or interface segments that require efficient data in motion security. Diagram 2 shows a few of the target interfaces within the front-, mid-, and back-haul that HSE can address. However, because it is a security capability, HSE is not bound to any physical or virtualized network constraints. The HSE is protocol-agnostic, it can be implemented through Layer 2, Layer 3, and Layer 4 architectures. Its unique rules-based implementation allows HSE to secure diverse layers and traffic types simultaneously through a single endpoint. There is no longer a need to implement protocol-specific data in motion security solutions that are tied to the network layer. The Thales HSE brings together unparalleled data in motion security and performance through wired, wireless, and software defined networks.



5G Target Pathways requiring high levels of security and performance

Install and connect in modern networks

Copper, fiber, wireless, virtual, and software defined networks are all supported from speeds of 10 Mbps to 100 Gbps. Virtual endpoints provide for east-west data protection within the data center, virtual private cloud (VPC) to VPC connectivity within the cloud, and 100 Gbps data center to data center connectivity. From front-haul to mid-haul to back-haul, HSE can secure data flows throughout the 5G network.

Separation of Duties

Solutions like IPsec have a drastic effect on performance that often results in security being sacrificed for performance to accommodate the end-user experience. HSE separates the network management functions from security functions, ensuring both compliance and performance are properly managed. Since the HSE does not adversely affect performance, the end-user experience is greatly enhanced and management burdens are reduced. The elimination of third party certificate authorities means that the MNOs retain complete auditable control of the Data In Motion security. This level of security control can effect auditability for GDPR, HIPA, Schrems II, and other data export compliance requirements.

Custom development

Although HSE can be deployed as physical, high-performance hardware, the virtual HSE can extend to security endpoints including bare metal servers, virtual infrastructures, cloud endpoints (VPCs), and hardware integrations.

Always know the whereabouts of your keys

HSE does not require third party certificate authorities. Instead, the Root of Trust resides with the owner of the data or the operator of the network. Complete, auditable chain of custody for the key material is maintained between all physical and virtual segments in which the data may travel. Once the Root of Trust is established, the HSE acts in a simple "set it and forget it" mode with complete control over the key lifecycle management.

Crypto agility

Next generation 5G networks require crypto agility to ensure data in motion security protects the network well into the future. HSE has AES256 encryption today as well as all of the down selected quantum algorithms for future compliance. HSE hardware can leverage Quantum Random Number Generation (QRNG) and provides APIs for integration with Quantum Key Delivery (QKD) solutions. Completely field upgradeable, HSE secures today and well into the future without the need for forklift replacements.

Meet your compliance needs

Whatever your compliance needs may be, HSE has been designed to meet the most stringent global standards. HSE hardware solutions meet FIPS 140-2 Level 3, Common Criteria EAL4, ANSI, and NATO certifications. With tens of thousands of endpoints globally deployed in more than 35 countries, HSE is a proven data in motion security solutions for government, defense, and commercial markets worldwide.

Thales can help

Address 5G security network vulnerabilities from the edge to the RAN and core with HSE. Contact us to learn how to quickly adapt your infrastructure to meet 5G performance, scalability, speed, cost and privacy requirements for 5G, and establish a root of trust for your critical data links.

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