cpl.thalesgroup.com

celona | THALES
Building a future we can all trust

Secure Private Wireless Solution

High Performance Private 5G with Transparent, Quantum Safe Security for Data in Motion

White Paper

Overview

As organizations are looking for a high coverage of predictable and secure wireless, existing technologies are not able to keep up. Celona and Thales have combined their private LTE/5G solution and High Speed Encryption (HSE) solution respectively to create a unique, highly reliable, secure wireless connectivity solution – especially for use cases where predicable throughput, low latency and security are critical. The Thales network encryptors are FIPS 140-2 L3, Common Criteria (CC) certified and are already used by governments for various applications worldwide. It delivers maximum uptime and near-zero latency for the most demanding, performance intensive environments. Together with the turnkey solution from Celona, organizations can very quickly deploy a high performance, low latency, private cellular network that leverages all the benefits of 5G performance and security while ensuring data privacy, residency, and the ability to integrate with existing access and application QoS policies.

Celona's private wireless solution featuring patented MicroSlicingTM delivers predictable performance to a new generation of critical enterprise, industrial and defense applications. When coupled with Thales' award-winning HSE solution, customers retain the inherent performance benefits of 5G infrastructure and gain the assurance of FIPS level encryption technology.

This secure wireless solution can be used in cloud and data center services, government information and secrets, commercially sensitive data, intellectual property, defense and military information, business and financial data, banking transactions, CCTV networks and more.

Celona 5G LAN Solution

For decades, companies have relied on wireless technologies including microwave, satellite – and specifically Wi-Fi, for wireless backhaul and access connectivity. While these technologies have helped us radically transform our networks, they do have limitations that business-critical applications will expose.

Some common examples of challenges and their impact are noted below:

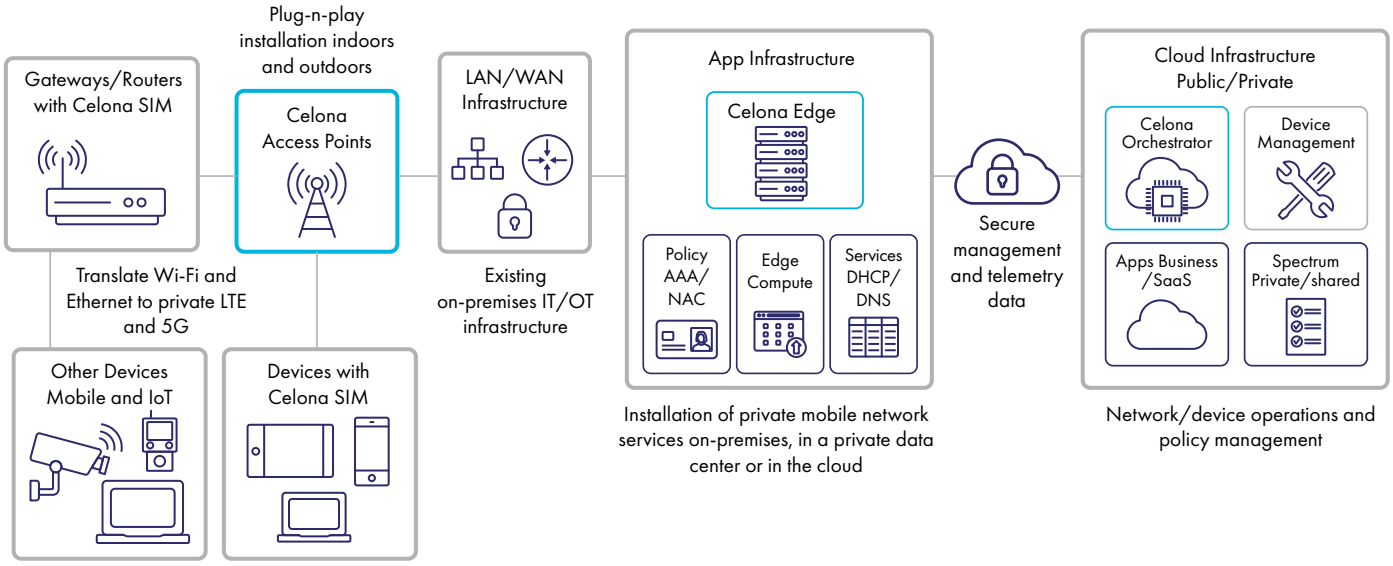
Wireless Challenge	Coverage Deficiencies	Quality of Service	Mobility	Data Security
Enteprise Impact	Weak signal strength and dead spots prevent device connectivity	Inability to define latency and throughput service levels beyond QoS prioritization	Performance dependent on client devices as they roam between wireless APs	IoT devices often do not support highest form of Wi-Fi security

Private 5G cellular technology have intrinsic capabilities (like higher power levels, and centrally scheduled media access protocols) that can help organizations overcome these limitations. However traditional solutions are often cost prohibitive and succumb to inherent deficiencies in being able to seamlessly integrate with enterprise networks and policies. Developed as an IT-friendly overlay atop existing enterprise networks, Celona 5G LANs provide a flexible and easy to use alternative to these traditional private cellular solutions.

Celona Private 5G Solution Overview

Celona's integrated 5G LAN platform includes all the essential elements including access points, LTE/5G core network edge hardware/ software and cloud-based orchestration tools specifically designed and developed for enterprise network use-cases. As opposed to traditional solutions, a private 5G LAN allows for enterprises to have full control over company data with a predictable long-term cost structure.

The components that make up a Celona RAN include enterprise-optimized **Celona indoor/ outdoor access points (APs)** that operate in private cellular spectrum, **Celona Edge** software as the extension of the Celona platform integrated to existing enterprise network infrastructures, the cloud-managed **Celona Orchestrator** and physical SIM or embedded SIM (eSIM) cards.



The Celona Edge element of the overall Celona integrated platform is the **private mobile core and control plane** for the software-defined RAN. All data is directed through the edge platform – allowing for complete control and visibility of the data flows traversing the RAN and to allow for the application of various network services.

The Celona Edge acts as the gateway connecting the LTE/5G cellular wireless to corporate LAN resources. Support for NAT, static/ dynamic routing and VLAN connectivity are possible in its ability to integrate with existing IP domains and enterprise network traffic forwarding requirements. Deployable either on-premises or within a public or private edge/cloud, the Celona Edge performs the following data-plane functions:

- Cellular radio spectrum management and data plane services for Celona APs
- Application performance and telemetry metric data collection
- User/device access control and data security

The Celona Orchestrator is responsible for the centralized control of:

- Celona AP and Celona Edge auto-provisioning, ongoing management
- User equipment (UE) onboarding, offboarding, device grouping via SIM provisioning
- Celona MicroSlicingTM policy creation and management for app QoS and service levels
- Cellular wireless visibility and monitoring of real-time performance against MicroSlicingTM policies
- User management including support for Single Sign On (SSO) and Role Based Access Controls (RBAC)

The Celona 5G AP specifications are noted below:

Overview	MIMO: 4 x 4 Channel Bandwidth: 20/40/60/80/100 Mhz
Throughput (100 MHz)	1 Gbps DL (3D1U configuration) 600 Mbps UL (3U1D configuration)
Throughput (40 Mhz)	400 Mbps DL (3D1U configuration) 250 Mbps UL (3U1D configuration)
Number of connected devices	400 active
Latency	< 15ms roundtrip (software roadmap to ultra-low latency)
Other	Modulation:256 QAM, SCS:30KHz EIRP: 37 dBm (per port), 13-18dBi ant. gain IP67 rated

5G LAN QoS with MicroSlicing

Within a Celona 5G LAN, QoS policies can be created for a mix of applications across different device groups using Celona's patented MicroSlicing™ technology.

There is no need to manually touch client devices for MicroSlicing™ policies to be applied, and the policies can be changed in real-time as application and device mixes within a Celona 5G LAN evolve over time.

A MicroSlicing™ policy is defined as a set of network functions within the Celona 5G LAN that form an end-to-end logical policy fabric. A single policy can be configured to meet an application's network performance requirements with service level objectives on flow priority, packet delay budget (aka. latency), packet error rate (PER) and bandwidth.

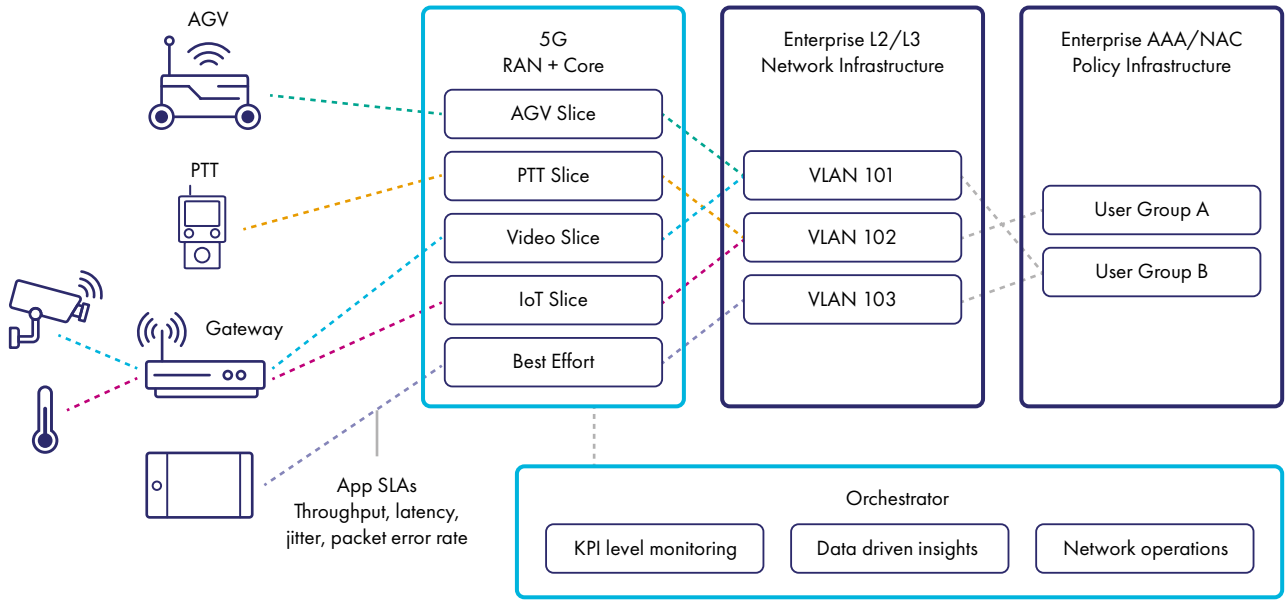
The control plane of a Celona 5G LAN continuously monitors and adjusts traffic transmissions

to meet such service level objectives. These processes and functions guarantee deterministic performance of critical enterprise applications when on private cellular – in addition to ensuring that QoS rules for higher-priority traffic over lower-priority flows are enforced in real-time.

Accordingly, within the Celona 5G LAN, in addition to simply prioritizing one traffic flow over the other, each traffic flow is monitored for latency, error rate and throughput within the Celona Orchestrator – on device group and application basis. Here is a quick summary of each:

Device groups – Administrators can group cellular wireless endpoints via their SIM identities into specific groups and logically segment them by device type or use case. In many scenarios, the type of device often dictates what apps/services are being operated on a regular basis. This helps to coordinate which devices are assigned which MicroSlicingTM policy.

Applications – Applications can be configured based on server IP / subnet mask and start/end ports. Once defined, the application flows are identified by the Celona platform in real-time as client devices connect. Once a combination of device groups and application types are married to specific MicroSlicingTM policy, service level objectives are enforced.



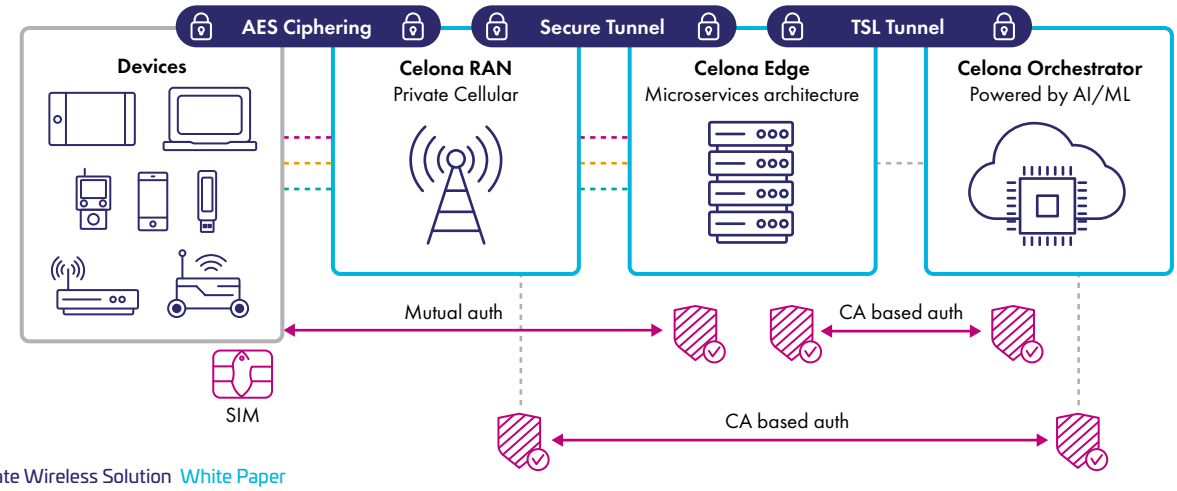
QoS policies can also be maintained when transporting data between the Celona network and the corporate LAN. Each MicroSlicingTM policy within the Celona 5G LAN can be assigned with dedicated DSCP markings to translate cellular wireless service level requirements to traditional QoS enforcement on the enterprise network. QoS policy can then be created around these DSCP tags on the wired network to provide preferential treatment to mission-critical application flows using queuing, forwarding and discarding mechanisms such as traffic shaping or traffic policing.

Celona's platform has been designed with enterprise administrators in mind. From an IT operations standpoint, Celona has taken great care to help enterprise network operations, cybersecurity and service delivery teams feel comfortable configuring and monitoring a private cellular wireless infrastructure. Taking cues from popular cloud-managed enterprise wired, SD- WAN and Wi-Fi solutions, concepts found in Celona's operational model will prove to be similar and accessible to administrators from different parts of the IT organization.

5G LAN Security in Celona Solution

5G LANs offer clear benefits over alternative wireless solutions. Data security is one area where clear advantages can be seen. Unlike Wi-Fi security which has evolved over time and introduces the chance of insecure misconfigurations, only the latest and best security mechanisms are built directly into the cellular wireless connectivity. Thus, network administrators do not have to concern themselves with the thought of accidently deploying a wireless network using inferior authentication and encryption mechanisms.

A private 5G LAN provides highest levels of enterprise wireless security with regards to authentication, authorization, and encryption. The use and management of X.509 public key certificates are not required as proof of endpoint identity as this process within the Celona 5G LAN is handled with the identification information contained within the SIM card assigned to a specific device. There is no SSID or network name or network password for the end user or the network administrator needs to provision – and the policies of when, where, and how that specific SIM card could be provided network access can be defined via software, in real-time, based on logical policies.



User/device authentication and access control within a 5G LAN are designed to adhere to zero trust philosophies and frameworks. Of course, device identification and authentication are two key tenants of zero trust principles. With the use of physical or digital SIM cards that secure store subscriber identities, devices without the proper SIM identification information will never be able to join the 5G LAN.

Finally, as described earlier, application flows can be placed into secure Celona MicroSlicingTM policies where each device group and application mix per policy can be safely isolated from all other traffic traversing the 5G LAN.

In addition to the inherent security benefits of 5G solution – and the value-add capabilities that Celona delivers on top – the Thales HSE solution delivers an added layer of security and performance capabilities to support highly demanding, mission critical applications. The HSE solution from Thales is described in more detail below.

Enhanced Security using Thales HSE

5G networks have unique requirements for both security and performance. From signaling and control plane data to the end-user experience, efficient use of bandwidth, low latency, and low jitter are non-negotiable mandates. In addition, the sheer network scale, number of edge clients, and the heightened potential for a range of attacks including network attacks, risks regarding legacy networks and protocols, and component and supply chain risks all emphasize the need for greater security without compromise. Bottom line: 25-year-old security solutions, such as IPsec, are not equipped to meet the security and performance for these next generation 5G networks. Modern networks and applications need security solutions with low latency, negligible jitter, and maximized throughput to deliver on the promise of 5G which includes greater security, bandwidth and responsiveness to the edge.

Thales High Speed Encryptors (HSE) encryption devices are built to meet the exponential growth of data streams 5G will facilitate and trusted to protect network-transmitted data in more than fifty countries globally.

5G Security and Network Performance

5G use cases are widespread and varied. For example, the requirements for secure data delivery of a driverless car can be quite different from the requirements of an enterprise data center backup, a small office vital link, or the Mobile Network Operator's backhaul control plane data. The diversity of packet sizes, protocols, and transport layers make consistency in security and performance impossible using traditional security methods. IPsec has not changed much since implemented back in the 1990s, it is far from qualified for 5G for the following reasons:

- Bandwidth - IPsec overhead can consume up to up to 50% of the bandwidth on smaller frame sizes
- Latency - IPsec Increases latency and jitter by milliseconds, eating up a substantial percentage of 5G latency budget
- Security – Limited key management control, lack of crypto agility and quantum safe security makes it vulnerable to modern threats

A major problem with older security solutions is that security is closely tied to the transport layer. IPsec is added to devices like routers and firewalls for purposes of convenience. Aside from the obvious overhead inefficiency required at the transport layer, these multi-function devices are using processing power to make transport, routing, and filtering decisions for each frame. The additional burden of encrypting and decrypting each packet injects overall poor performance in terms of throughput, latency, and jitter. As devices are patch and more capabilities are added, these all-in-one devices slow down over time particularly when security patches and upgrades are applied to meet emerging standards.

Thales Transport Independent Mode (TIM)

Separating security functions from the transport layer improves security and eliminates performance constraints. With Transport Independent Mode, Thales encryptors concurrently encrypt data at Layers 2, 3, and 4 of the network providing flow diversity and efficiency. This mode eliminates the constraints of performing all encryption at a single layer or the overhead of managing multiple protocols. This tunnel-less approach does not add overhead but rather utilizes a NIST approved crypto offset to allow for end-to-end encryption

By separating security controls from the transport layer, a security overlay is provided allowing the network elements to optimize routing and switching decisions. This simple separation of security from transport provides control over key management, auditable end-to-end security, separation of duties, and quantum safe data transport at the highest levels of performance. Thales HSEs provide real-time encryption techniques that can meet requirements from 1Gbps edge clients to 100 Gbps backhaul and core infrastructures.

Thales HSE's use an efficient scalable encryption protocol that is designed for modern networks. This approach overcomes many of the inherent limitations of standard MACsec and IPsec and delivers significant performance benefits.

Thales High Speed Encryption	Traditional IPSec Encryption
Any to any connectivity	Point to point or hub-spoke only
High scalability	Exponentially complex @ scale
Low latency efficient tunnel free encryption	High overhead and bottleneck for traffic
High availability	Manual failover proceduers
Flexible policies giving transparent encryption ay differnet layers	One size fits all encryption with many network dependencies

Performance Comparisons

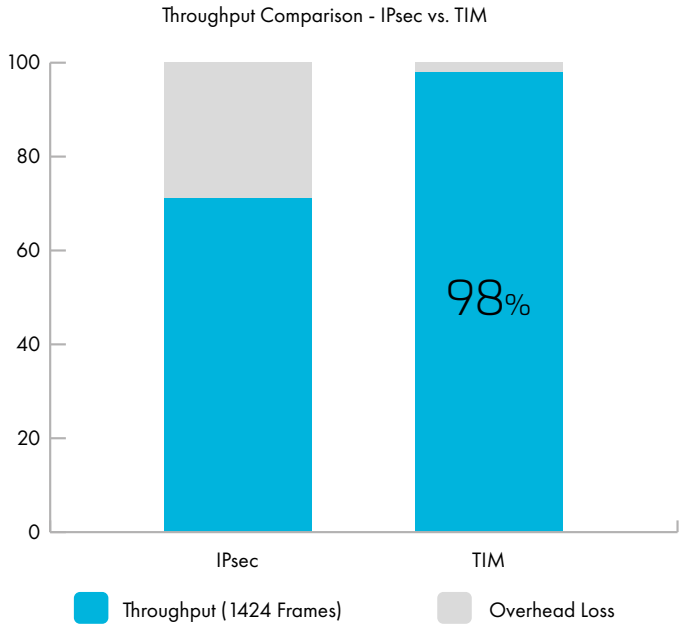
Highest security/maximum performance

The results below represent lab test results when comparing and off the shelf IPsec device to a Thales HSE. These test were run against identical network configurations and traffic profiles.

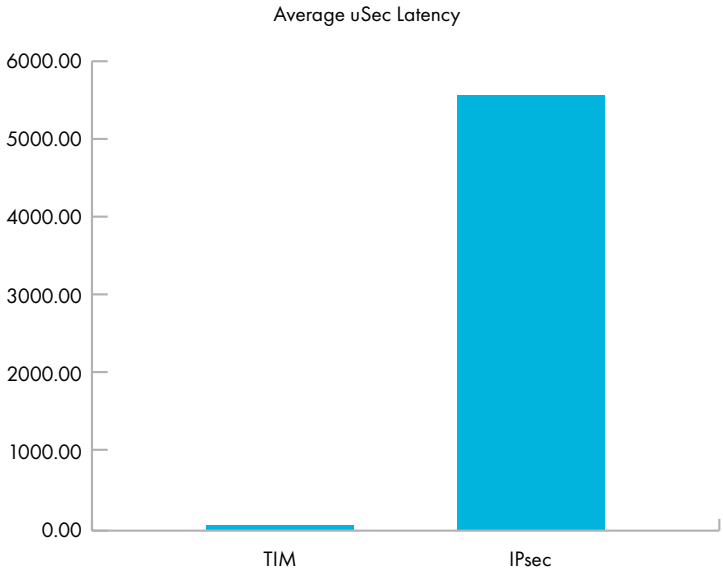
The real-life scenario of average performing IPsec devices highlights the dramatic affects that packet size and processing power have on overall performance. Although the IPsec manufacturer claims 1Gbps IPsec performance, this claim can only be achieved under very specific test conditions, leveraging higher performing devices at the end point, while using aggregated WAN connections. This scenario is not only costly, but unlikely to exist in real-world field deployments.

The figures below clearly shows the dramatic throughput difference between IPsec and the Thales TIM implementation. These results compare an off the shelf IPSec encrypt IPsec achieved only 71% total performance under the device's best-case, optimized environment. The processing power (and price) of the IPsec endpoints as well the diversity in packet sizes provides for additional negative impact on performance. Smaller packets, such as voice and video, require the same amount of overhead as larger data packets. The result is a greater ratio of overhead to data.

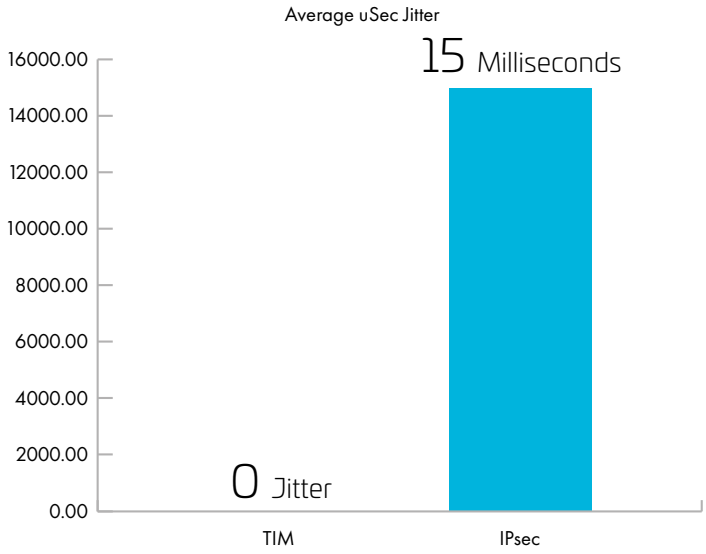
Thales High Speed Encryptors with TIM consistently outperform legacy IPsec with Latency (see figure 1), Jitter (see figure 2) and overall performance (see figure 3) below.



IPsec vs. Thales Transport Independent Mode

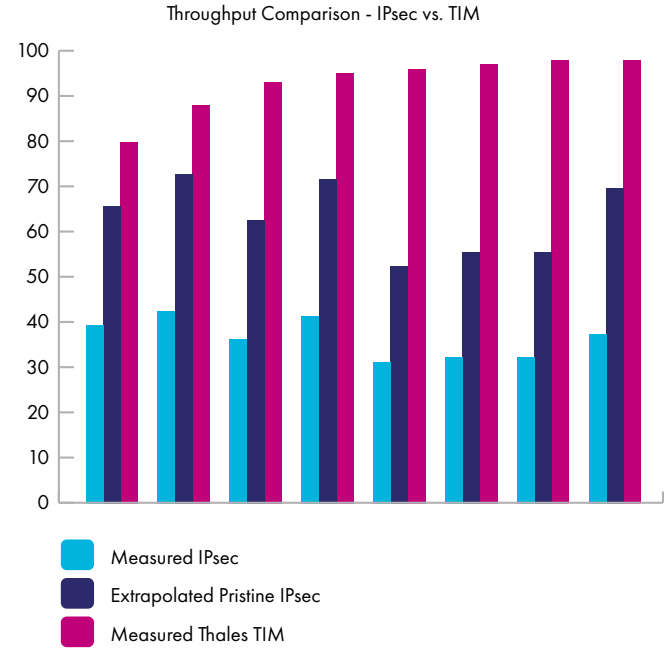


IPsec vs. Thales TIM Latency over a 5G Infrastructure



IPsec vs. Thales TIM Jitter over a 5G Infrastructure

It is expected that higher-perming IPsec devices will produce better results however, pristine conditions yielded a best case of only 71% performance for IPsec. Based on these idealized, theoretical conditions, we can extrapolate expected results. In comparison to TIM, it is clear that consistency of performance over diverse network conditions can be achieved. In addition it shows the drawbacks and dangers of assuming the optimized results vs testing against real world traffic scenarios.



Measured IPsec vs. Extrapolated Pristine IPsec vs. Thales 1G HSE with TIM

Separation of Duties

One cannot discuss the importance of separating security from the transport layer without identifying the benefits of separation of duties. Access to security controls should be limited, monitored, and audited by a group that dedicates itself to standards implementation and compliance, while allowing network administrators to tune the network. This ensures a high quality of network performance while preserving the integrity of the security. The Thales TIM feature provides protocol agnostic security with little to no impact on network performance and ensures that both high levels of security and performance are independent of each other even when provided as a packaged solution.

Thales encryptors provide full-line rate encryption at speeds up to 100 Gbps with ultra-low latency and close to zero jitter using a non-blocking cut-through encrypted data path.

The design of Thales encryptors has been independently assessed by multiple third-party certification labs around the world and the platform has the broadest range of independent certifications available on the market including:

- FIPS 140-2 Level 3
- Common Criteria EAL2/4+
- DoD APL
- NATO Restricted
- ASD ISM

HSE provides a fully certified & compliant encrypted overlay that is independent of the network function and delivers best practice separation of duties that isolates security management from device management. HSE is available in a variety of form factors including optimized hardware encryption appliances and a variety of software implementations (e.g. VNF, CNF etc). The key benefits include:

- Performance that is independent of application type or traffic mix
- Tunnel free encryption delivers higher throughput and lower latency
- FIPS 140-2 Level 3 physical security - tamper proof, anti-probing protection
- Crypto-agile, future proof in-field upgradeable appliances
- Quantum safe key management

Thales encryptors are simple to use and manage. They provide the following capabilities:

- Set & forget device installation
- "Bump in the wire" transparent encryption operation
- Out of band, in-line or in-band device management
- Fully automatic key management

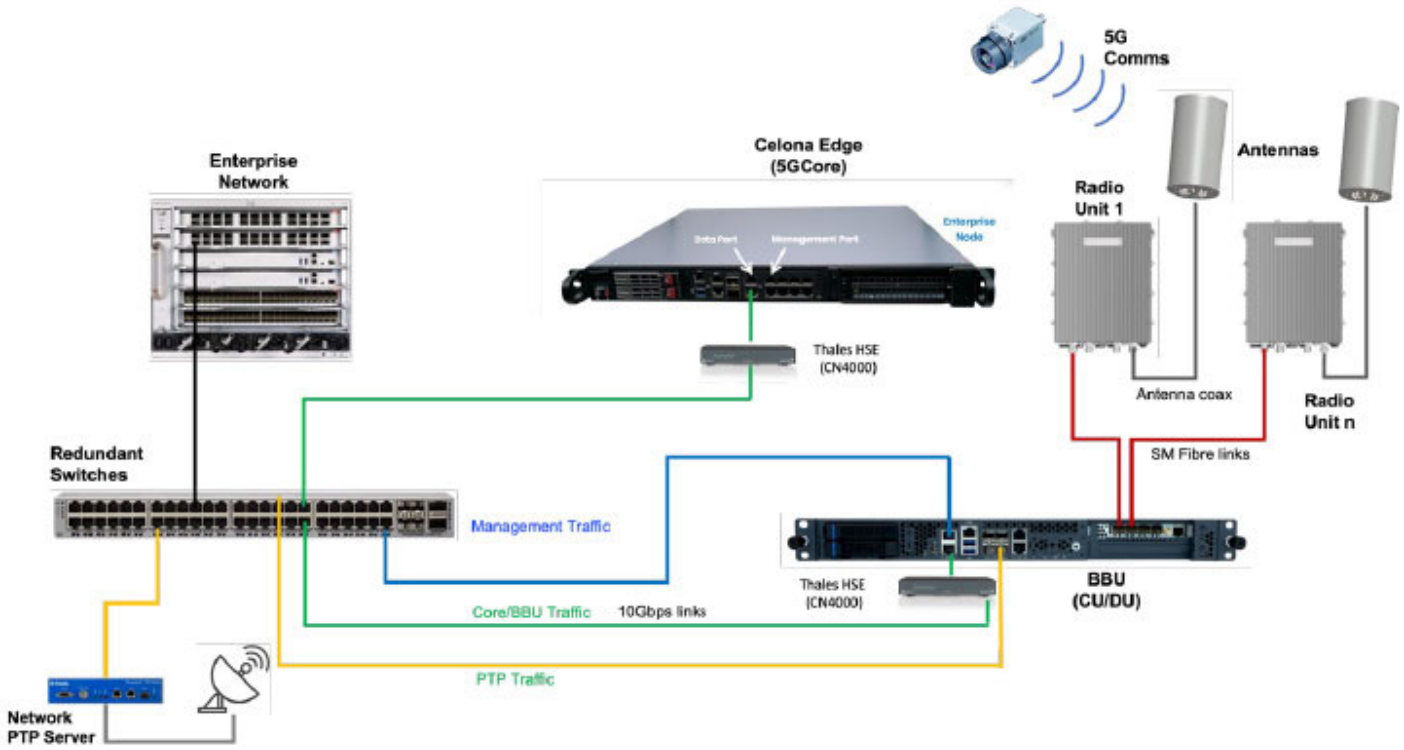
Thales HSE devices have implemented quantum safe security in advance of the formal NIST Post-Quantum Cryptography standards as follows:

- Support for hybrid dual certificates to allow hybrid classic/PQC key establishment across layer 2 networks
- Support for connections to ETSI-014 QKD standard appliance

Celona and Thales Key Development Milestones (Summary)

Phase 1:

Proof of Concept (PoC_ solution deployed using the end to end Celona 5G LAN solution and Thales HSE using dedicated hardware encryptors (as shown in the following diagram):



Phase 2:

Thales encryption modules ported to Celona BBU and Celona Edge hardware to deliver a fully integrated solution

Summary

Celona and Thales are partnering to create the industry's leading solution for the most secure, high performance private 5G solution that can benefit a wide spectrum of industries including government and defense.

By combining modern access point technology and the latest advancements in security organizations can take advantage of the full range of 5G benefits including:

- Performance and reliability
- Future proofed, high-assurance data in motion security
- Data and operational control of a private 5G network

THALES

Building a future we can all trust

Contact us

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

> cpl.thalesgroup.com <