Case Study

THALES

CYBERSECURITY

Sovereign Defence Supplier Secures Mission-Critical Data in Motion

With Certified Thales High Speed Encryptors

cpl.thalesgroup.com

THALES

CYBERSECURITY

About the Organization

A global provider of defence and aerospace was commissioned by a European government agency that needed to securely connect data centres and protect sensitive information moving between sites.

The data being transmitted was of critical national importance. It required high-assurance protection, strong operational controls, and encryption capable of supporting demanding sovereign defence security requirements.

For this customer, the objective was not simply to encrypt traffic. It needed to reduce the risk of mission-sensitive data exposure, compliance failure, operational disruption, and loss of control over sovereign information flows.

Challenges

Protecting sovereign data without compromising performance or control

The defence supplier needed to protect mission-critical data in motion between two data centres while maintaining the performance, availability, and resilience required for sovereign defence operations.

Network links may be vulnerable to interception, tapping, or manipulation, so the customer required dedicated encryption to protect sensitive traffic end to end. The solution also needed to be decoupled from the underlying network architecture, so encryption could remain independent of any specific topology, protocol, or network vendor environment.

A key requirement was separation of duties. Encryption could not simply be treated as another network function managed through routine network operations. The customer needed dedicated controls to help ensure that encryption policy could not be disabled, bypassed, or weakened without proper authorisation.

The solution also needed independently validated security assurance, including FIPS 140-3 Level 3 and Common Criteria EAL4+ certifications, to support procurement, compliance, and accreditation requirements. Performance was equally important: encryption had to operate at full line rate with minimal latency, so mission-critical services would not be slowed or disrupted.

Industry

Sovereign Defence

Location

Europe

Use Case

Secure data-centre interconnect

Solution

Thales High Speed Encryptors - CN6140 Multilink Network Encryptors

Security Assurance

FIPS 140-3 Level 3; Common Criteria EAL4+, PQC-ready, supporting all NIST-standardized Quantum Resistant Algorithms

Deployment Environment

Supported deployment across RESTRICTED and SECRET environments

Deployment

Certified, high-assurance encryption between data centres

The defence supplier selected Thales High Speed Encryptors to protect data in motion between the two data centres. The deployment used Thales CN6140 Multilink Network Encryptors, providing transparent, PQC-ready, high-assurance encryption at full line-rate speeds up to 4x 10 Gbps.

Certified Security and High-Performance Encryption

The deployment combined independently validated security assurance with the performance, flexibility, and operational control required for mission-critical defence operations.

- FIPS 140-3 Level 3 validated cryptographic protection
- Common Criteria EAL4+ certified security
- Supported deployment across RESTRICTED and SECRET environments
- Full line-rate encryption up to 4x 10 Gbps
- Low latency of less than 6µS
- Standards-based AES-256 encryption
- End-to-end authenticated encryption
- Secure client-side key storage and automated key management
- Transport Independent Mode across Layers 2, 3, and 4
- Zero protocol overhead mode to maximise available bandwidth
- 1U appliance form factor for efficient data-centre deployment

The CN6140 platform is designed for high-speed data-centre and network connectivity environments where performance and assurance are both essential. Using Field Programmable, Gate Array, FPGA, technology, the CN6140 architecture enables real-time data processing, high throughput, and consistent low latency across packet sizes.

Thales High Speed Encryptors are purpose-engineered for dedicated network data security. The selected solution provided secure, tamper-resistant hardware dedicated to network encryption, standards-based cryptography, authenticated encryption, and secure key management with client-side key storage.

The platform's certified security architecture and flexible configuration supported deployment across both RESTRICTED and SECRET environments. This allowed the customer to use a consistent encryption platform across different classification levels, helping reduce capital expenditure, simplify operations, and standardise security controls.

Adding the Thales High Speed Encryptors to the existing network was straightforward due to the bump-in-the-wire design of the appliances and their interoperability. This allowed seamless integration without the unnecessary network redesign while maintaining control over encryption policy, independently from the underlying network infrastructure.

Thales High Speed Encryptors also support Transport Independent Mode (TIM) which provides network-layer-independent data-in-motion encryption across Layers 2, 3, and 4. This protocol-agnostic approach gave the customer flexibility to protect traffic across different network designs, routing architectures, and future deployment scenarios.

HSE operates with automated key management designed to reduce ongoing operational effort after initial configuration. Unlike approaches that may require manual transport or installation of physical key material, the solution manages the lifecycle of secret session keys without ongoing user intervention.

The platform's FPGA-based architecture and HSE design also support crypto-agility and field upgradeability, providing a path to adapt to evolving cryptographic requirements, including future standards and customer-controlled entropy options where required.

Results

Secure, resilient data flow for sovereign defence operations

The defence supplier was able to protect sensitive data moving between data centres while maintaining the performance required for mission-critical defence operations.

By encrypting data in motion, the customer reduced the risk of sensitive information being exposed or manipulated if network traffic was intercepted. Built-in integrity protection and authenticated encryption helped ensure that unauthorised or altered traffic would not be accepted as trusted communication.

The ability to support both RESTRICTED and SECRET environments created significant business value. Rather than deploying and managing separate encryption technologies for different classification levels, the customer could use a consistent, certified encryption platform across multiple sensitive environments. This reduced capital expenditure, simplified operations, and helped standardise security controls.

Automated key management further reduced operational burden by eliminating the need for ongoing manual key handling or physical key material transport after initial configuration.

The customer also gained a more controlled and auditable approach to network encryption. By separating encryption from routine network administration, the organisation strengthened its ability to enforce security policy, reduce bypass risk, and maintain control over sensitive sovereign data flows.

The deployment also supported operational resilience. In the customer's network design, traffic could be redirected over an alternate secure path to help maintain availability in the event of a network issue or suspected compromise.

The result was a high-assurance, high-performance encryption deployment that protected sovereign data in motion, supported accreditation requirements, reduced operational complexity, and provided flexibility for future network and cryptographic requirements.

About Thales

Thales is a global leader in cybersecurity, helping the most trusted organizations protect critical applications, data, identities, and software anywhere, at scale. Through Thales' integrated platforms, customers achieve better visibility of risks, defend against cyber threats, close compliance gaps, and deliver trusted digital experiences for billions of consumers every day.

Contact us – For contact information, please visit cpl.thalesgroup.com/contact-us

© Thales - June 2026 • AC v2