

Thales End-To-End Encryption Solutions: Securing Government Data



Contents

3 Securing Government Data

- 3 Why Encrypt
- 3 Protection Vs. Prevention

4 Trusted by Governments in more than 20 Countries

- 4 Maximum Data Protection Without Compromise
- 4 Government Customers

5 Choosing the right Encryption Solution

6 End-to-End Encryption Solutions

- 6 Thales CNSeries Hardware Encryptors
- 6 Thales CV Series Virtualized Encryptor
- 6 Suredrop Encrypted File-Sharing

7 What makes Thales encryptors stand out?

- 7 Best Performance
- 7 High-Assurance

8 Network Independent Encryption

- 8 Versatile & Simple
- 9 Low cost, high efficiency

9 About Thales

Securing Government Data



The sensitive nature of much of the data held by local and central government agencies places a greater-than-average emphasis on effective cyber-security.

Protecting everything from citizen data to state secrets requires a holistic approach; one that includes both prevention and protection solutions for data at rest and in motion.

Historically, there has been an emphasis on prevention technologies – a combination of physical and virtual. However, if the past decade has taught us anything it is that data breaches are inevitable.

In recent years the accidental loss of data has lessened slightly, but still accounts for one third of all lost or stolen records. The primary source of data breaches is the malicious outsider, or “hacker”. In 2019, 52% of breaches featured hacking, 28% involved malware and 32–33% included phishing or social engineering, respectively.

Why Encrypt?

The rapid growth of virtualization, data center and cloud computing technologies mean we are becoming increasingly reliant on our highspeed/high-availability data networks to deliver information when and where we need it.

Cyber-crime in the form of hacking, corporate espionage and even cyber terrorism, is on the rise. Information security threats remain commonplace and there is an increasing emphasis on organizations of all types to ensure the integrity and security of their data, both at rest and in motion.

We cannot rely on the assumption that our data remains secure within the perimeter of the office environment. All organizations share systems and information that rely upon common network access and most modern businesses comprise multiple offices, some separated by a few yards, others by thousands of miles.

Fibre-optic cables are used to transport petabytes of data across private and public networks every day. Although still considered the fastest and most reliable method of moving data, Fibre networks have become increasingly vulnerable as hacking technologies become more sophisticated, less expensive and more readily available.

Protection Vs. Prevention

There is a common misconception within many organizations that a robust firewall is enough to prevent unwanted access to their network. Unfortunately, this is not the case.

While the firewall can detect and eliminate a variety of penetration or denial of service attacks, it is no protection against a physical tap either inside or outside the firewall.

The only fail-safe solution to ensure that your data is secure as it travels across the network is encryption. Furthermore, your encryption solution should be de-coupled from any specific network architecture and accredited against recognised world-wide security standards.

Trusted by Governments in more than 20 Countries

Thales certified high-assurance encryptors are specialist hardware products; dedicated to protecting sensitive government information transmitted across high-speed data networks - without compromising network performance.

Thales hardware encryptors provide government departments and agencies with the peace of mind that comes from certification by multiple, independent testing authorities. They are certified suitable for Government and defense use by FIPS, Common Criteria and NATO.

Certification involves years of rigorous testing by the testing authorities' own labs. Without these certifications, products are unable to be installed in the respective government data networks.

In addition to our encryptors' certifications, government and defense customers have also undertaken their own proof of concept and benchmarking testing. In every case, Thales encryptors have excelled.

Importantly, organizations providing services to the government and defence sectors – such as Cloud computing or data center storage services – can meet the certification requirements of their own government customers by using Thales certified high-assurance products.

That assurance of multiple certifications is one important reason why Thales encryptors protect much of the world's most sensitive data and are a first choice of government departments and defense forces around the world.

In addition to long-term data integrity and security, Thales encryptors provide governments with protection from:

- Data 'sniffing' or eavesdropping
- Data theft or redirection
- Input of rogue data
- Loss of intellectual property
- Privacy breaches or identity theft
- Loss of trust or reputation
- Financial loss or penalties
- Breach of compliance obligations
- Innocent human and technical errors

Maximum Data Protection Without Compromise

Thales encryptors provide maximum security without compromising network performance.

Unlike other 'low-assurance' alternatives, they do not add network overhead or expose network links to unnecessary vulnerabilities.

They are used by governments in more than 20 countries to protect sensitive data essential to a wide range of applications, including:

- Cloud Computing
- Big Data Capture and Analytics
- Data Center Back-Up and Disaster Recovery
- CCTV Networks

Government Customers

Thales encryptors are used to secure network transmitted data for a wide range of government and defense organizations.

Among those that mandate Common Criteria, NATO or FIPS certification, Thales encryptors are used by:

- Government agencies – law enforcement, service agencies, regulatory bodies, etc.
- National defense and military
- Cross-government agency and departments data-sharing
- Telecommunications carriers network services provided to governments carriers'
- Cloud computing and data center services increasing use by governments
- Inter and intra-office data networks

Choosing the right Encryption Solution

A lack of vendor compatibility within the network encryption marketplace means organizations looking to secure both core IT infrastructure and virtualized WAN need to think carefully about a choice of technology.

When it comes to choosing an encryption vendor, it's important to consider all the possible applications. Just as important is the realization that all encryption solutions are not created equal.

As recommended by leading data security and encryption analysts; for a network encryption solution to be truly robust and provide long-term data protection (well beyond the useful life of the data), it must be a "high-assurance" solution.

So-called 'hybrid' encryption devices – such as network routers/switches with embedded encryption or those using MACSec or similar standards (not originally intended for WAN and MAN security) provide "low assurance" data protection.

By contrast, Thales CN Series network encryption solutions are certified by the world's leading independent testing authorities as suitable for government and defense applications. They are purpose-engineered for dedicated, highassurance network data security.

Thales network encryptors' security credentials include all four, essential highassurance features:

- Secure, tamper-proof hardware; dedicated to network data encryption
- State-of-the-art encryption key management; featuring secure, client-side key storage
- End-to-end, authenticated encryption
- Standards-based encryption algorithms

For real-time data applications, latency is a significant issue. While adding a network encryption interface card to an existing switch may seem like an attractive option; it will result in higher latency and lower throughput performance than a dedicated Layer 2 device.

In some instances, using an NIC means the same vendor needs to be used throughout the network route and that data is decrypted and re-encrypted at each of the "hops".

This is both a security risk and a major key management issue. Dedicated appliances enable data to remain encrypted throughout the network route, irrespective of switch vendor.

If an NIC is used, the lifespan of the encryptor will be tied to the host network device and will need to be replaced when the switch is changed.

Most modern infrastructure comprises multiple network Layers; typically featuring Layer 2, 3 and 4 elements. So, organizations should look for a vendor that provides Layer agnostic encryption where possible.

Thales' CV Series virtual appliances provide concurrent, multi-Layer encryption and support DPDK for up to 5Gbps performance.

Like the CN Series hardware encryptors, our virtual appliances support all topologies, from P2P to Hub & Spoke and fully meshed networks.

End-to-End Encryption Solutions

Thales CN Series Hardware Encryptors

The CN Series of network encryptors provide certified, high-assurance data protection for core IT and communications network infrastructure.

All CN Series encryptors share a common encryption platform and are 100% compatible and interoperable.

The CN Series of hardware encryptors are used to secure sensitive data in motion across networks operating at anything from modest 10 Mbps to ultra-fast 100 Gbps bandwidths.



CN4000

Small form-factor (desktop) encryptors for 'in the field' network link security (e.g. CCTV) – offering 10 Mbps, 100 Mbps and 1 Gbps bandwidth speeds.



CN6000

Rack-mounted high speed encryptors for business-critical applications – offering 1 Gbps to 10 Gbps bandwidth speeds.



CN9000

Ultra-high bandwidth, rack-mounted encryptor with mega-data performance – offering speeds of up to 100 Gbps.

Thales CV Series Virtualized Encryptor

The CV1000 virtual encryptor provides strong and effective data encryption for large-scale and virtualized wide-area networks.

Scalable to thousands of end-points, the CV series of virtual encryptors is a software application of the trusted Thales encryption platform. It delivers cost-effective, transport Layer agnostic data protection at up to 5 Gbps (with DPDK).

As a Virtualised Network Function (VNF) that will run on any x86 hardware, the CV Series virtual encryptor is 100% interoperable with Thales CN Series hardware encryptors and is built on FIPS compliant technology.

Suredrop Encrypted File-Sharing

SureDrop delivers the file-sharing convenience of popular box-style applications, but with the addition of end-to-end encryption security and 100% data location control.

It also offers users a choice of the resilience of a bespoke, on-premises solution or the flexibility of a managed service provider solution.

SureDrop clients include government agencies and service providers that are concerned about the inherent risks associated with sharing documents outside of their protected LAN.

SureDrop represents a new way to enjoy secure file sharing; with the emphasis on delivering a service that meets the needs of large commercial and government organizations who are required to frequently share sensitive and confidential information across the web.

SureDrop also provides organizations with the user authentication security benefits of active directory compatibility.

What makes Thales encryptors stand out?



Best Performance

High-Speed

The designed-in, market-leading performance capabilities of Thales encryptors are what make them stand out from the crowd.

Whether operating at 10 Mbps, 100 Mbps, 1 Gbps, 10 Gbps or 100 Gbps; time after time, they consistently win competitive performance tests.

Their encryption speeds, near-zero data overhead and near-zero latency make Thales encryptors ideally suited to the most demanding network environments.

Ultra-Low Latency

Thales high-speed encryptors operate in full duplex mode at full line speed 99.99% without loss of packets.

Latency is not affected by packet size (<2 microseconds per unit at 10 Gbps) meaning maximum throughput with near zero protocol overhead.

Importantly, by using Field Programmable Gate Array (FPGA) technology, this outstanding performance is predictable and dependable.

Near-Zero Impact

The zero impact of Thales encryptors is not limited to network bandwidth and latency; it extends to network operations and management.

They simply fit in within the user network. They don't require changes to other devices or network reorganization; making them a favourite among network engineers.



High-Assurance

Certification In-Depth

Because Thales CN Series encryptors include the only multi-certified products of their types, they are trusted by governments and defense forces around the world.

Rigorous testing is carried out over many years and provides our government and commercial customers with maximum confidence. Thales CN Series encryptors are certified by: FIPS, Common Criteria and NATO.

For 20 years, Thales R&D has included a commitment to certification in depth. Customers value the benefits of exhaustive and ongoing testing authorities' product evaluation.

Best Encryption Key Management

All Thales products adopt state-of-the-art encryption key management. Your encryption keys are only ever held by and accessible to you, on your premises; securely stored and encrypted.

Solution Integrity

Thales encryptors provide maximum solution integrity; unlike 'low assurance' solutions, such as router-based network data encryption or so called 'hybrid' encryptors.

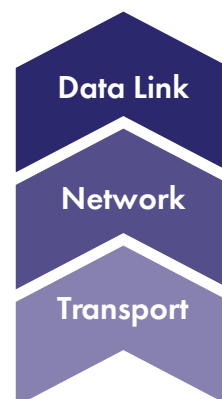
Thales high-assurance encryption solutions feature dedicated, tamper-proof hardware and provide gapless, end-to-end, authenticated encryption with standards-based (AES256) encryption algorithms.

Network Independent Encryption

Many organizations utilize multiple data network Layer protocols (Layer 2, 3 and 4) to help deliver their business applications and communications services. Recognizing this, Thales has designed-in Network Independent Encryption.

This advanced, network Layer agnostic encryption technology enables destination policy-based, concurrent multi-Layer encryption.

Significantly, customers are still assured of strong, end-to-end encryption as the protected data traverses the various network Layers, for example: from Layer 2 Ethernet to Layer 3 IP network destination.



Versatile & Simple

CRYPTO-AGILITY

All Thales encryptors are crypto-agile; from 100% compatibility and interoperability to customisable encryption and FPGA based flexibility. Selected Thales encryptors also support Quantum Key Distribution (Quantum Cryptography) and Quantum Random Number Generation, for long-term data security.

SUPPORT FOR ALL PROTOCOLS

The Thales CN range of encryptors provides the widest feature-set. Able to operate at 10Mbps to 100 Gbps, they are designed for Layer 2 Carrier Ethernet WAN and MAN networks and support all Layer 2 protocols: Ethernet, Fibre Channel; SONET/SDH and LINK.

SUPPORT FOR ALL TOPOLOGIES

Thales CN encryptors operate in point-to-point, point-to-multipoint and fully meshed network topologies. Thales CN9000 encryptors are the only 100 Gbps encryptors that support multipoint-to-multipoint topologies.

CUSTOM ENCRYPTION

In addition to the standards-based AES256 and 128-bit algorithms, Thales CN encryptors support the use of customer-requested algorithms, custom curves (BYOC) and entropy (BYOE).

EASE OF USE

Set and forget simplicity and network transparency are underlying Thales design themes. They ensure ease of implementation, operation and management. All Thales encryptors feature automatic zero-touch key management. They also feature automatic network discovery and connection.

INTEROPERABILITY

Thales encryptors supporting the same Layer 2 network protocol are fully interoperable. All Thales CN models are backward compatible.

LOCAL OR CENTRALISED MANAGEMENT

Configuration may be performed locally or remotely through the intuitive Thales CM7 management software; which acts as the Certificate Authority in a network of encryptors by signing and distributing X.509 certificates.



Low cost, high efficiency

Suitability

All Thales CN encryptors operate at full line speed; enable maximum network performance and deliver set and forget management simplicity.

The business investment case out-performs even cheap and cheerful low-assurance solutions that prove very costly over time.

It is not necessary, nor beneficial, to opt for low cost, low-assurance solutions to meet the toughest business case and TCO requirements.

Cost-Efficiency

Thales encryptors provide excellent total cost of ownership through a mix of network bandwidth savings, ease of management and reliability.

Longevity, interoperability, backward compatibility, minimal installation and management costs and solution flexibility all contribute to a rapid return on investment.

Other cost benefits include, low power consumption minimal rack space use and combined rack space/power utilization efficiency.

Reliability

99.999% uptime and conform to international requirements for safety and environment. All carrier-grade, rack mounted Thales encryptors are hot-swappable and provide further network operations up-time benefits thanks to dual redundancy of encryptor consumables such as fans and power supplies.

Unlike hybrid encryptors and other low-assurance solutions, network up-time is not disrupted by Thales encryptors.

Flexibility

Thales encryptors' use of FPGA technology enables maximum operational flexibility. They are better able to meet customers' specific requirements and provide an optimized highspeed data encryption solution.

This flexibility enables on-going operational simplicity, such as infield upgradability, as customers' requirements change; helping to protect their investment in technology.

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.



Contact us

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

> cpl.thalesgroup.com <

