cpl.thalesgroup.com

THALES

Securing financial services network data

White Paper

Contents

Compliance & Obligation

Financial services is one of the most tightly regulated business sectors. The FSA, the Data Protection Act, GDPR, PCI/DSS and Euro SOX all have implications for securing financial data in transit.

Personal data is a valuable commodity. Most financial institutions will hold extensive personal and financial data on their customers, including names, addresses, dates of birth, bank account details, PINs and passwords. Ironically, a lot of this data is held to ensure secure identification of customers in the first place.

Financial organizations often have a robust business continuity plan that involves secure off-site backup and disaster recovery. However, it is during this process that data becomes most vulnerable. Whilst individuals' personal or financial data may be secure, other information that forms a part of the backup and recovery process, such as internal email, often aren't.

A financial institution's responsibility to data security doesn't end at the front door. They are also responsible for the data when it is shared with a third party. No matter how secure your internal policies and practices, once your data is traversing the public network, it's vulnerable.

Understanding Financial Services

Financial services is one of the most tightly regulated sectors in business. The FSA, the GDPR, PCI DSS and Euro Sox all have implications for the security of information in transit.

Thales has been working with our global resellers and OEM partners to deliver encryption solutions to the financial services sector for more than a decade. During this time we have helped secure WAN and data center infrastructures for a variety of banks, trading houses and asset management companies.

Why Encrypt?

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

Cybercrime in the form of hacking, corporate espionage and even cyberterrorism, 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.

High-speed access is also an essential part of business continuity as it enables a robust back-up and disaster recovery strategy.

Financial data is a prime target for theft, with retail and financial institutions being hit hardest of all. High profile breaches targeting financial data at JP Morgan Chase, Home Depot, Target, Adobe, HSBC, Carphone Warehouse and others have hit the headlines in recent years.

Banking and financial services are amongst the most tightly regulated industries. The sensitive nature of the data held at rest and transmitted across their networks places an emphasis on IT security.

However, the time-sensitive nature of transactional data means that any stringent data security policies, procedures or technologies cannot come with an additional network overhead. When dealing with large scale transactions, every nanosecond counts.

These exacting standards require high-performance, low-latency solutions to ensure security, availability and profitability.

Network Vulnerability

Petabytes of data are transmitted across private and public networks every day. While still considered a fast and reliable method of moving data, core network infrastructure has become increasingly vulnerable as bad actors expand the type, volume and frequency of their attacks.

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.

High-Performance, Low-Latency Solutions

Thales has a legacy of designing and developing solutions tailored to the specific requirements of the global banking and financial services industry. Our state-of-the-art high-assurance encryption solutions allow organizations to remotely provision and manage global WAN security as easily as they would their LAN or data center connections.

Our solutions are among the most rigorously tested and certified in the world, meeting the internationally recognized standards of FIPS, Common Criteria, CAPS and NATO; ensuring both physical security and best-practice encryption key management.

Provisioning and management of encryption devices, either locally or remotely, is quick and easy. Set and forget functionality means minimal ongoing maintenance and advanced monitoring tools allow for real-time alerts or reporting for audits, compliance and forensics.

Choosing the Optimal Encryption Solution

Due to a lack of vendor compatibility in network encryption, organizations need to find a vendor that offers a complete range of products; one that is able to cover all their network encryption needs and provide 100% compatibility for all protocols and topologies.

Despite the obvious variation in customer requirements, one thing is certain today - if you are serious about protecting data networks; any encryption solution less than high-assurance is a wasted investment.

There are many encryption solutions on offer; but only a very small number that offer high-assurance considerations, such as:

Performance

Adding a network encryption interface card to an existing switch will appear attractive, however there will be a higher latency and lower throughput performance than a dedicated Layer 2 encryption device.

This is especially relevant in high-speed data center and disaster recovery links running at gigabit speeds over fibre, transmitting small packets such as voice and video.

Lifespan

If a network encryption interface card (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.

Management

In some instances, using an NIC will mean the same switch vendor is needed through the network route and will result in the data being decrypted and re-encrypted at each of the "hops". This is a potential security risk and will be a major key management issue. Dedicated appliances will enable the data to be encrypted the whole route, irrespective of switch vendor.

Certification

Many switch and encryption vendors are not approved to encryption standards such as Common Criteria, NATO or FIPS. Thales encryptors are independently tested and accredited by the world's leading testing authorities and offer the only multi-certified encryption solution.

Why High-Assurance?

To be considered a high-assurance encryptor, it must: be a secure dedicated hardware device; enable end-to-end encryption; use state-of-the-art encryption key management and hold international certification.

Quantum Key Distribution

Quantum Key Distribution (QKD) is a technology that relies upon two fundamental principles of quantum physics to generate encryption keys. Firstly, that the generation of the quantum key is truly random and secondly, that any attempt to interrupt or eavesdrop on the encrypted data will disturb the system and be detected.

Unlike classical encryption key generation, which is based on mathematical algorithms, QKD will not become compromised as computing power increases. More importantly, it is not vulnerable to passive attacks, where data is captured for subsequent decryption. Passive attacks are potentially the most dangerous for financial services organizations as they often go undetected until the data has been decrypted and the consequences felt by the business.

In a passive attack, data is typically copied or captured and stored offline for future decryption – either through brute force attacks or when current PKS algorithms are broken. Data such as customers' financial, credit card or personal details have long-term relevance for identity theft or fraud, so longer-term protection is essential.

The Thales and QKD integrated solution has been successfully deployed in a number of major European financial institutions, providing forward-secrecy for the most sensitive long-term data.

Whilst the current state of the technology is limited in terms of distance, banks and asset management companies are utilising QKD to secure 10 GB network connections, as a part of their back-up and business continuity strategies, to disaster recovery sites up to 100 KM away. Outside of real-life applications, QKD has been successfully demonstrated in laboratory conditions over distances as great as 300 KM.

However, the future of long-distance QKD is likely to come in the form of satellite-based key exchange, with low-orbit communications satellites transmitting keys securely to a network of terrestrial base-stations.

Why Quantum Key Distribution?

QKD solutions provide the ultimate in quantum-safe security for long-term data protection.

By harnessing the power of quantum mechanics, QKD ensures a provably secure key exchange, alerting to any potential eavesdropping, as well as providing forward secrecy of the encryption keys.

Combining Hardware and Virtualized Encryption

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.

The choice between hardware and virtualized encryption is based on an organization's individual needs and preferences. Often, it is not a case of either/or – but a blend of the two technologies together.

Security Versus Performance and Network Link Use

Hardware encryptors deliver predetermined high-performance, not able to be matched by software/virtualized encryption. They also provide maximum data security through multi-certified, high-assurance credentials.

Network Link Use Cases

High-speed links (>5 Gbps) are more commonly used to connect IT infrastructure such as data center interconnects, or Big Data feeds.

Encrypting data in motion between branch locations is of equal importance, though network speeds will vary between these locations.

These links ideally require both maximum data protection and best performance, only offered by hardware encryptors.

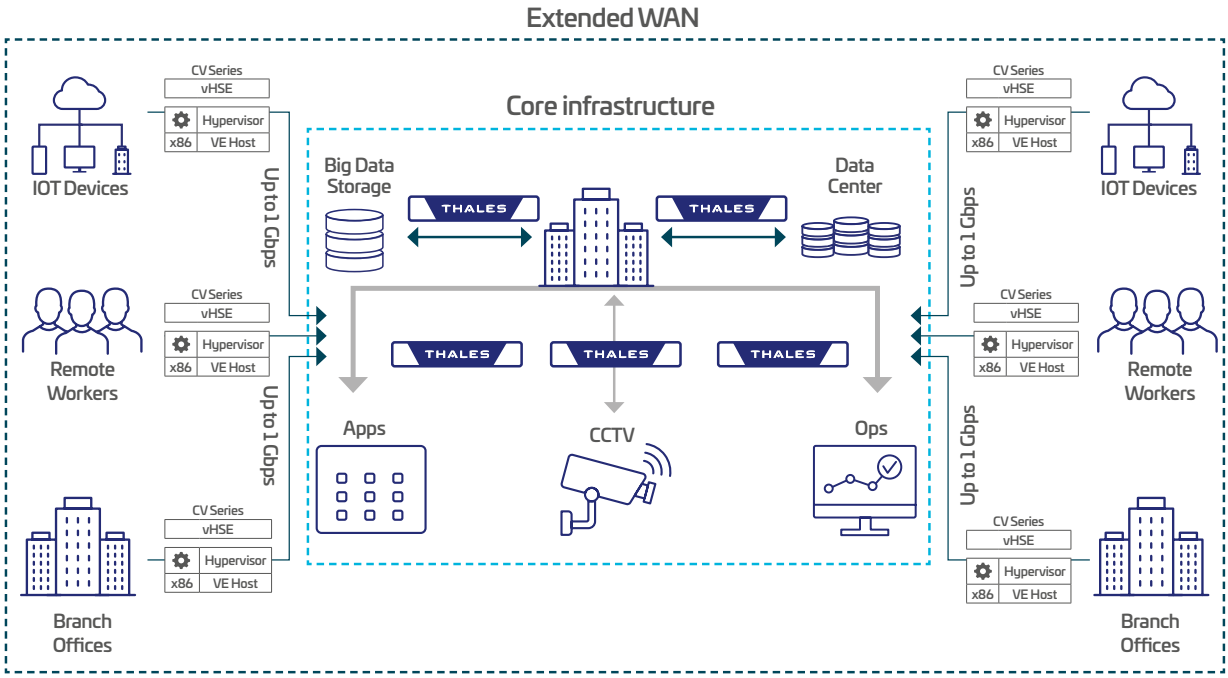
However, for extended WAN links and high-scale virtualized links that typically run at up to 5 Gbps, a virtual encryptor is likely to be a more flexible and cost-effective solution.

Mixed Use Cases

Organizations often only deploy hardware encryption to protect core IT infrastructure data in motion. Many operate unprotected extended WAN links.

Virtualized encryption provides an opportunity to encrypt all data in motion through a single compatible technology.

Ultimately, organizations should use dedicated hardware encryption for their main feeds, interconnects and branch locations, while virtualized encryption is used to provide scalable, cost-effective encryption for devices at the network edge.



CN Series Hardware Encryption

CN9000 Series

The CN9100 is the world's first commercially available certified high-assurance 100 Gbps network encryptor that supports all network topologies.

Like all Thales CN encryptors, the CN9000 Series provides maximum high-assurance network data security, without compromising network and application performance. It boasts ultra-low latency of just 1.5 microseconds in customer testing.

Developed in collaboration with customers and service providers, Thales CN9100 encryptors are designed to meet the exacting requirements of all 100 Gbps use cases, making them an ideal application for securing public and private Cloud networks.

Thales' CN and CV Series encryptors include integrated support for CipherTrust Key Manager (Thales' centralised cryptographic key management solution) that provides maximum security for the storage of master keys, the integrity of security policies and the source of entropy for the generation of cryptographic keys.

CN6000 Series

Thales CN6000 Series encryptors provide highly secure, full line-rate transparent encryption for data moving across both dark fibre and metro/wide area Ethernet networks; in point-to-point, hub & spoke or meshed environments.

The CN6000 Series are rack-mounted, high-speed encryptors for business-critical applications; offering 1 Gbps to 10 Gbps bandwidth speeds. They are the optimal choice when you require:

- Efficient, investment-proof data encryption
- Multi-purpose, in-field upgradable and flexible hardware
- Choice of Common Criteria, and FIPS certifications
- Compact 1U form factor with advanced performance and power features

CN4000 Series

As network security is a challenge to organizations of all shapes and sizes, Thales also provides a series of compact encryptors - the CN4000 series - to help address the encryption demands of smaller organizations and in-field operations.

Despite their small form-factor, Thales CN4000 Series encryptors boast the same robust security credentials of their rack-mounted cousins.

The CN4000 series is the ideal low-cost, high-performance encryptor range for small to medium-sized enterprises (SME). They also provide a cost-effective encrypt everywhere solution for larger enterprises looking to secure remote or temporary locations connected via networks operating at up to 1 Gbps.

Like all CN hardware encryptors, the CN4000 Series features standards-based encryption, secure key management and the peace of mind that comes from certification by the world's leading independent testing authorities.

What Makes CN Series Encryptors Stand Out?

Performance

High Speed

Market-leading performance. Operating anywhere from 10 Mbps or 100 Gbps, Thales encryptors consistently win competitive performance test.

Low Latency

Operating in full duplex mode, at full line speed, without packet loss. Latency is as low as 2 microseconds per unit at 100 Gbps.

Zero Impact

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

Versatility

Crypto Agility

All Thales encryptors are crypto-agile; from 100% compatibility and interoperability to customizable encryption and FPGA based flexibility.

Topology Support

Thales CN encryptors operate in point-to-point, point-to-multipoint and fully meshed network topologies.

Flexible Management

Configuration may be performed locally or remotely through the intuitive Thales CM7 management software.

Security

Certification

For more than 20 years, Thales R&D has remained committed to the principle of certification in depth. Thales CN Series encryptors are certified by: FIPS, Common Criteria and NATO.

Key Management

All CN Series encryptors feature state-of-the-art encryption key management. Keys are securely stored and encrypted, and only accessible by you.

Solution Integrity

Thales high-assurance encryption solutions feature dedicated, tamper-proof hardware and provide gapless, end-to-end, authenticated encryption.

Efficiency

Cost Effectiveness

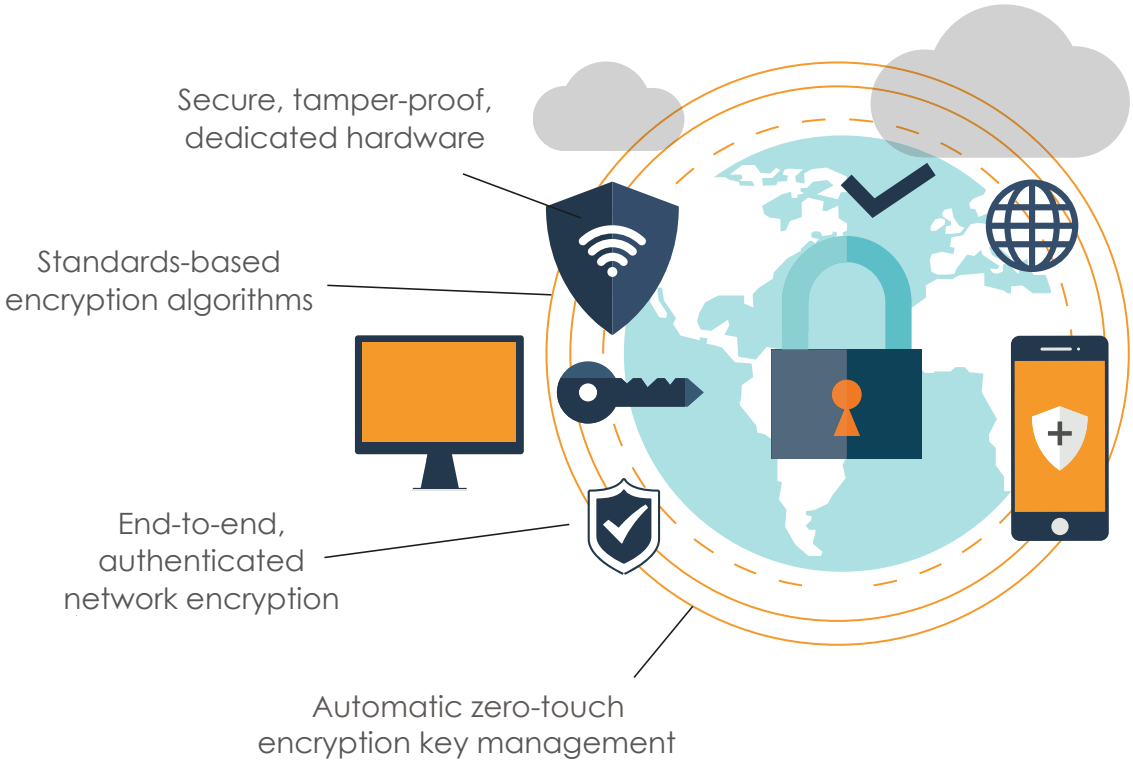
Thales encryptors provide excellent TCO through a mix of network bandwidth savings, ease of management and longevity.

Reliability

All carrier-grade Thales encryptors are hot-swappable, feature dual redundancy and deliver 99.999% uptime.

Flexibility

Use of FPGA technology enables maximum operational flexibility, including use of custom encryption and in-field upgradability.



High-Assurance Encryption

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.

Not all encryption solutions are created equal. 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 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, high-assurance network data security.

Thales CN Series encryptors' security credentials include all four essential high-assurance features:

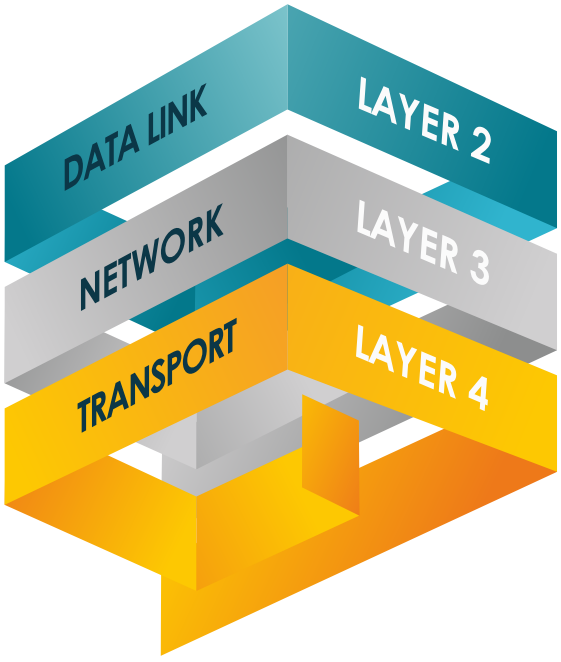
- Secure, tamper-proof hardware; dedicated to network data encryption
- State-of-the-art, client-side, zero-touch encryption key management
- End-to-end, authenticated encryption
- Use of standards-based encryption algorithms

Network Independent Encryption

Many organizations use 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.



CV1000 Virtualized Encryption

The CV1000 is a Virtual Network Function (VNF) appliance providing strong and effective data encryption security with designed-in crypto-agility. Designed for virtual CPE, the CV1000 delivers transport-Layer agnostic encryption for high-speed networks at up to 5 Gbps.

As an VNF appliance, the CV1000 stands out from the crowd. Instant scalability means it may be deployed rapidly across thousands of network links. It delivers the same flexibility and scalability as other virtualised network functions.

The CV1000 offers state-of-the-art encryption security and key management without impacting on network or application performance*. Unlike IPSec-type encryption solutions, the CV1000 is transparent to the network; making it ideal for securing your WAN, right to the virtual edge.

Integrated support for CipherTrust Key Manager (Thales' centralized cryptographic key management solution) provides maximum security for the storage of master keys, the integrity of security policies and the source of entropy for the generation of cryptographic keys.

Enhanced Key Security

The CV1000 is fully compatible with CipherTrust Key Manager; the industry's leading centralized key management platform.

Available as a hardware appliance or a hardened virtual security appliance, CipherTrust Key Manager provides support for multiple key types: symmetric, asymmetric, secret data and X.509 certificates.

CipherTrust Key Manager simplifies the management of encryption keys across the entire life-cycle; including key generation, storage, backup, distribution, deactivation and deletion.

DPDK acceleration - performance up to 15 Gbps

DPDK Intel libraries enable x86 host device performance acceleration. If the host x86 device and DPDK are optimally configured, the CV1000 will deliver enhanced performance of >1 Gbps up to 5 Gbps.

Consistent performance up to 15 Gbps is dependent upon host configuration and expertise in DPDK setup and configuration.

Environment and architecture factors may also play a role in virtualized encryption performance, as they do in virtualized networks.

Key Benefits

Unmatched benefits of the CV1000 expressed by end-user customers and service providers include:

- The CV1000 enables adoption of a virtualized encryption solution that does not compromise on security or network and application performance
- Instant scalability to match the scale and flexibility of virtual and software-defined networks
- No requirement to deploy large numbers of hardware encryption devices to achieve high scale implementation of network encryption
- The CV1000 encryption security and key management model is optimized for strong and effective encryption security
- Through Transport Independent Mode, the CV1000 is suited to a multi-Layer network environment
- Competitively, the CV1000 delivers up to 30% network performance benefit over other solutions
- Ease of deployment with centralized, zero touch provisioning
- 100% interoperability with Thales CN Series encryptors
- As a software implementation of the Thales high-assurance encryption platform, the CV1000 provides a flexible, cost-effective way to encrypt all the way to the virtual edge
- Data center service providers identified the CV1000 as an optimal solution; providing strong and effective encryption security among devices within the data center itself

SureDrop Encrypted File Sharing

No matter where or how the people in your organization work, there is always the need to share and sync files - both internally and externally.

While you want to enable collaboration, data security should always be the first priority. If it's not, the risk of non-compliance and data breaches become a serious problem.

Our customers have been telling us that their mobility and productivity initiatives are frustrated by insufficient levels of security delivered by existing box style file collaboration and sync and share solutions.

While many are user friendly, elegant and effective, they're simply not safe enough.

Thales provides SureDrop to deliver state-of-the-art, standards-based encryption algorithms, key management and 100% file control security - without comprising your user experience.

In design, features and functionality, SureDrop solves the security issue of convenient file-sharing and synchronization, to the highest standards required by governments and large enterprises.

Key Benefits

- Available on-premises or from the Cloud
- 100% control over data sovereignty
- Unlimited file size and types
- Standards-based encryption
- Effortless management and control

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.

THALES

Contact us

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

> cpl.thalesgroup.com <