cpl.thalesgroup.com

Building the Foundation of Digital Trust

Using Thales Luna HSMs to secure your next generation of digital transformation

White Paper

Contents

Overview

Digital transformation is driving companies to integrate digital technologies into their businesses in order to create new customer experiences, simplify work, change culture, and meet changing business and market requirements. A recent study found that 43% of companies are embracing digital transformation by either aggressively disrupting the markets they participate in or embedding digital capabilities that enable greater enterprise agility. Technologies such as cloud computing, artificial intelligence (AI), the Internet of Things (IoT), analytics, machine learning, and edge computing have enabled businesses to reimagine ways of creating value, connecting with customers, and improving asset performance.

Consider how our daily lives are impacted by digitalization. Salesforce.com, Netflix and Amazon.com have changed the way we interact with customers, enjoy entertainment, and purchase goods – all online. Companies like Twitter, Facebook, and Snap have changed the way we connect with each other and how advertisers promote their brands. New digitalization efforts have also enabled companies in more established industries, like healthcare, manufacturing, and energy, to transform the ways they serve their customers. They are leveraging IoT, 5G, and augmented reality (AR) to improve remote monitoring, maintenance and performance of their systems. Even the financial industry has created new payment and customer options built on cloud, AI, and blockchain technologies.

Digital transformation is certainly increasing the growth of connected devices, and with that comes the challenge of ensuring the security, privacy, safety and reliability of the underlying systems and information. Security has become much more complex as IoT and edge devices reside beyond the firewall in untrusted networks. Virtualized and containerized applications using VMware, Docker, LXC, and Kubernetes are more difficult to secure due to the way microservices and applications are developed, deployed and run in an extensively distributed mode. Defense-in-depth security approaches and purpose-built security solutions can help to protect these systems; however, companies often fail to adequately protect the digital keys and unique credentials on which modern digital security is built.

Hardware Security Modules (HSMs) are purpose made to secure critical data and digital identities by generating, managing and storing cryptographic keys and certificates, and performing digital signing, in a validated and certified hardware root of trust. For decades, HSMs have been used to encrypt data and both create and protect the cryptographic keys used to secure sensitive data and critical applications. These private keys – or secret keys – are used in conjunction with cryptographic algorithms to encrypt and decrypt information for operations such as secure authentication, encryption, and code signing. By performing cryptographic operations inside an HSM, an organization is protected, reducing the vulnerabilities brought about by storing keys with data, taking advantage of high entropy keys, and knowing the whereabouts of its keys at all times regardless of the environment. HSMs can also be used in conjunction with IoT device security, blockchain, 5G and containerization to improve the authentication assurance level and trustworthiness of the overall solution.

This white paper was written to help CIOs, CISOs, COOs, product managers, process engineers, and product security engineers understand how Thales Luna HSMs support a variety of well-known and emerging cybersecurity use cases. We will also examine how Luna HSMs help meet compliance needs, easily integrate with common 3rd party applications, and secure your infrastructure, network, devices, applications and data regardless of where they are located.

Securing the Next Generation of Digital Transformation

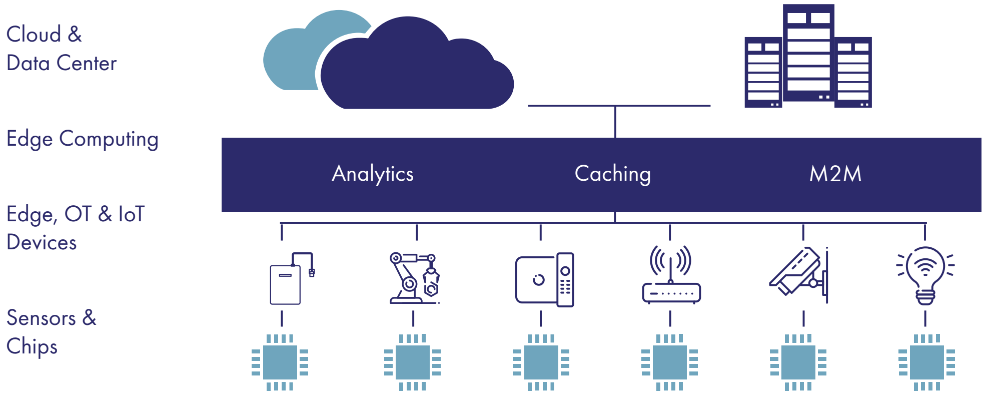

figure 1:
Cloud, IoT and Edge Computing

Source:
2020 Thales Data Threat Report
Global Edition

The next generation of digital transformation relies on cloud, IoT, and edge computing technologies. Securing the infrastructure, network, devices, applications and data across these systems is complex due to the differing constraints and operational models of each of these computing paradigms.

- **Cloud computing** leverages scalable computing resources, in the form of servers running in a data center, that perform the heavy lifting required by client applications running on a mobile or Internet-connected smart device.
- **IoT computing** shifts some of the processing to the device that can operate autonomously. These IoT devices are highly constrained by both processing power and memory, making them more difficult to secure than a smart device.
- **Edge computing**, the next generation of computing, shifts processing from the cloud to locations that are closer to IoT devices and endpoints to support applications that require low latency responsiveness, such as augmented and virtual reality (VR).

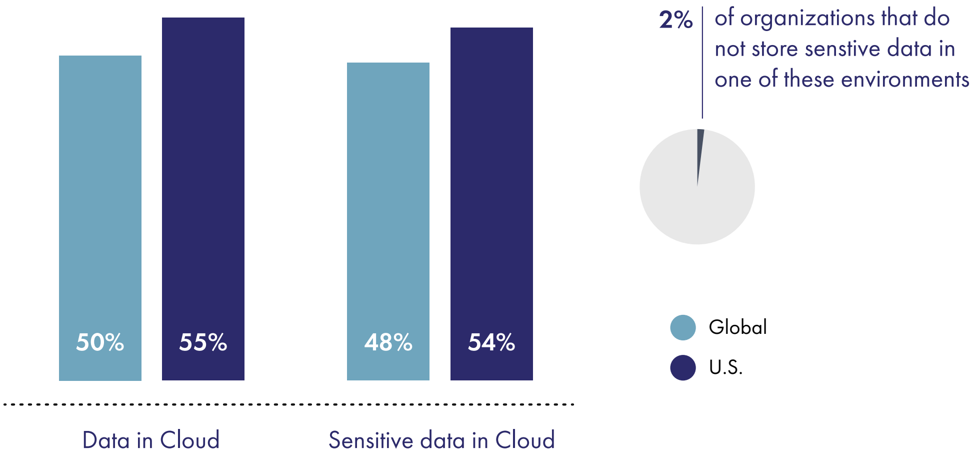

figure 2:
Data Stored in Cloud Environments

Source:
2020 Thales Data Threat

While organizations store half of their data in the cloud, 48% of this data is considered sensitive. Protecting modern enterprise and industrial systems is about more than simply protecting data-at-rest and data-in-motion. Enterprise servers, computers, mobile phones, smart devices, IoT devices, industrial control systems (ICS), applications, virtual machines, containers, and data all need to be protected from external and internal cyber-attacks.

Breaches are also impacting businesses. 49% of companies have experienced a breach at some point, and 26% reported being breached in the past year. Additionally, 47% of organizations report that they have been breached or failed a compliance audit in the past year.

To ensure the trustworthiness of a system, organizations must ensure that each of the components of a system have a truly unique digital credential, such as a private key, that is protected. Digital keys are the basis for authentication, encryption, and defense-in-depth security approaches. Using a key that can easily be compromised or derived allows attackers to steal private keys and impersonate devices or compromise other devices in the system.

Digital keys are used throughout the lifecycle of a device, application or virtual container.

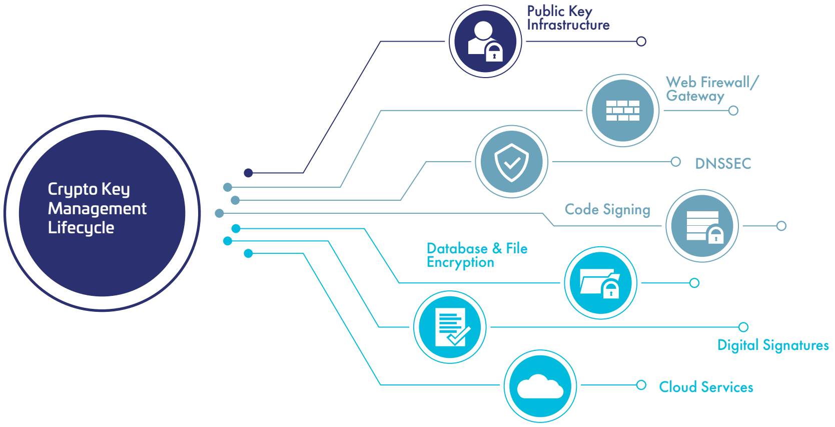
Crypto Key Management Lifecycle
Public Key Infrastructure
Web Firewall/ Gateway
DNSSEC
Code Signing
Database & File Encryption
Digital Signatures
Cloud Services

figure 3: Crypto Key Management Lifecycle

While many organizations use pre-shared keys (PSK) or manual key management, these methods can make it easier for hackers to compromise systems. For example, sending pre-shared keys and other private keys over the Internet may enable attackers to more easily steal those keys using phishing or eavesdropping attacks.

The most secure way of generating and storing private keys is to use a hardware security module (HSM). In fact, for organizations where failure is not an option, they are considered mandatory and built into compliance regulations.

Hardware Security Modules

A hardware security module (HSM) is a device containing a dedicated crypto processor that is specifically designed for the protection of the crypto key lifecycle. HSMs act as trust anchors that protect the cryptographic infrastructure of some of the most security-conscious organizations in the world by securely managing, processing, and storing cryptographic keys inside a tamper-resistant device.

Enterprises buy hardware security modules to protect transactions, identities, and applications, as HSMs excel at securing and storing cryptographic root keys and provisioning encryption, decryption, authentication, and digital signing services for a wide range of applications.

Thales Luna HSMs

Thales Luna General Purpose HSMs are available in a wide range of form factors and performance options:

Luna Network HSMs
Secure sensitive data and critical applications by storing, protecting and managing cryptographic keys in Luna Network HSMs - Thales' premium family of high-assurance, tamper-resistant, network-attached appliances offering market-leading performance. Meet compliance and audit needs for FIPS 140-2 Level 3, HIPAA, PCI-DSS, eIDAS, GDPR, and others, in highly-regulated industries including financial, healthcare and government.

Luna PCIe HSMs
Embedded PCIe high performance cryptographic processor provides high-assurance protection for encryption keys typically used by original equipment manufacturers (OEMs) to increase the authentication assurance level of their products.

Luna USB HSMs
Deliver industry leading key management in a portable appliance. The USB form factor makes this HSM an ideal option for offline key storage.

Luna Cloud HSM
A cloud-based platform with pay-as-you-go pricing that provides a wide range of cloud HSM and key management services through Data Protection on Demand (DPoD) with a simple online marketplace. With Luna Cloud HSM, there is no hardware to buy, and integration with other cloud-based applications and SaaS platforms is simple.

Crypto Command Center is a centralized crypto management platform that enables security officers and administrators to provision, monitor and control Luna Network HSMs. The management platform generates dynamic reports and alerts to improve visibility and reduce remediation time. Crypto Command Center can also be used by service providers to offer crypto-as-a-service.

Feature	Luna Network HSM	Luna PCIe HSM	Luna USB HSM	Luna Cloud HSM
Form Factor	1U appliance	Low profile PCIe card	8.5" (W) 1U appliance	Cloud service
Mean Time Between Failure (MTBF)	171,308 hrs	997,508 hrs	858,824 hrs	99.95% availability
API Support	PKCS#11, Java (JCA/JCE), Microsoft CAPi and CNG, OpenSSL, REST, Python, GO, .NET merge both			
Algorithm Support	Broad set of asymmetric and symmetric algorithms, including Suite B ciphers			
Random Number Generator	US NIST SP 800-90A compliant with CTR-DRBG			
Certifications	FIPS 140-2 Level 3; eIDAS, Common Criteria EAL4+OCSI, Brazil ITI , Singapore CC NITES		FIPS 140-2 Level 3	FIPS 140-2 Level 3
Licensing Model	Perpetual license plus maintenance and support			Pay-as-you-go pricing

figure 4: Thales Luna HSM Features

Thales Luna HSMs provide the foundation for securing private keys for whole host of applications.

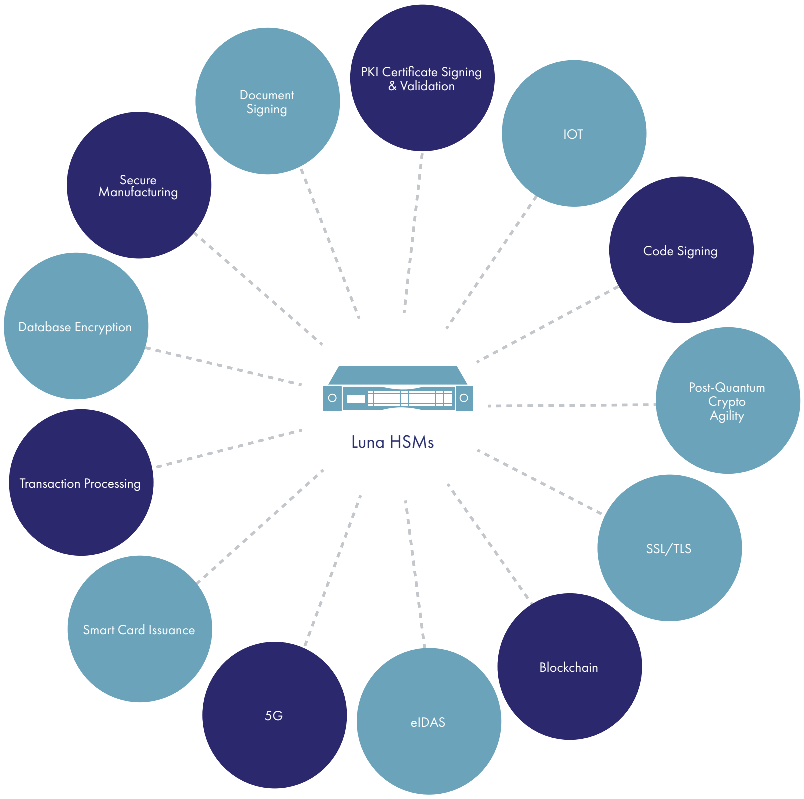

figure 5: Thales Luna HSM Traditional and Emerging Use Cases

Traditional Use Cases

In this next section, we will review a number of common use cases for an HSM.

A robust security solution is only as good as the ability to maintain proper confidentiality, availability, and integrity of the data which it protects. HSMs have been the foundation of trust anchors and roots of trust for many use cases where failure can have a detrimental impact and consequence to business operations.

Here are some examples where HSMs should be deployed in order to improve authentication assurance levels and ensure the utmost protection:

PKI

Public Key Infrastructure (PKI) is the cornerstone of modern certificate-based authentication. Effective PKI solutions utilize both public keys, which are shared somewhat freely with anyone wishing to engage in an authenticated transaction with another party, and private keys, which are never shared with anyone and are only held and managed by the root owner of the PKI system. It is critically important for the root private key to never be divulged or in any way altered, or the entire PKI can no longer be trusted. It is also very important the PKI is available any time an authentication request is presented. Failure in availability means the transaction basically halts in its tracks. Luna HSMs provide the foundational security needed to safely store and manage these keys.

TLS / SSL

Secure Sockets Layer (SSL) and its successor, Transport Layer Security (TLS) are the essence of secure communications over both public and private networks utilizing web-based protocols today. Today TLS has become the de facto standard for secure communications between two parties, particularly over the internet, but also within private networks which also rely on the same protocols. SSL and TLS require the negotiation of a secure connection that includes the dynamic generation of a shared key. In order to create the shared key, a private key must be used to generate it, and that is where an HSM is critically important. The HSM provides a robust environment to safely secure the key, as well as the critical horsepower to quickly generate and manage shared keys in environments where such keys need to be created and managed by the thousands and even millions every day. If an attacker can get a hold of the private keys, he or she can impersonate an organization, thereby destroying the trust.

Code Signing

Code Signing has quickly emerged in the connected world as a way to ensure users that the code they are running on their systems and devices is legitimate and has not been altered before getting onto their device, or even afterward. Over the last decade, code signing has seen widespread use in applications running on mobile devices and is now being utilized for code running on any device used in critical applications, such as medical devices, and control systems. In essence, code signing is the application of a digital signature to a piece of software by the creator of the software. In order to do this the code needs to be hashed, which is the generation of a small piece of data that represents the code and only the exact code that was hashed. This is verified in a checksum before the code is permitted to load and run on a device. In addition to the hash, the code is also provided with a unique digital certificate that identifies it as a product of the official creator of the code. Both the hash and digital certificate need to be verified by the device the code is run on. An HSM is deployed to generate and manage both the hash and the digital certificate that is used to sign the code, securing the critical code signing keys that verify the authenticity of applications, prevent tampering and man in the middle attacks, and protect against malware that can modify applications.

Modern code signing also includes a function known as Cloud Signing, where code can be uploaded via a secure TLS connection to a server that houses the private keys and hashing functions for the manufacturer in a secure environment deploying one or more HSMs, returning the signed code back to manufacturer over a secure TLS connection, which also deploys HSM functionality to ensure confidentiality, integrity and availability.

Database Encryption

One might say that PKI is the granddaddy use for HSMs, and database encryption, or encryption of large sets of data, is the grandma. As the world moved from the management of paper-based data to digital data over the last several decades, ensuring the confidentiality, integrity, and availability of the data with the ever-present threat of cyber-attacks is nearly impossible without a well-built, well-designed, and reliable HSM at the core of the system where the database resides. Without an HSM that is dedicated to the secure storage, management, and encryption of the database, business transactions would grind to a halt. It is important to keep in mind that both the encryption and decryption of large databases can be time consuming, and although some database systems do provide built-in encryption capabilities which protect stored data, if the cryptographic keys are in a software key vault then they are easy to compromise and tough to audit. The robust and scalable hardware solutions provided by the HSM enable organizations to handle database encryption efficiently and reliably.

Cloud, hybrid and multi-cloud

It is important to understand that only a few short years ago much of the functionality related to the above-mentioned use cases where (and still are) managed in closed environments, physically attended by organizational staff. Modern methods now utilize cloud-based infrastructure to offload such activities to organizations that are better equipped to manage such activities in the cloud. The server farms utilized in these cloud-based service provider environments rely on HSMs in order to ensure an organization and its clients that their data will not be compromised and be available when it is needed. The sheer number of threat actors attempting to compromise cloud-based service providers is staggering, and HSMs provide the peace of mind required by both the service providers and the clients they serve.

Emerging Use Cases

Digitalization has created new uses for emerging technologies, such as IoT, blockchain, quantum computing, and cloud native applications. While these technologies are being deployed, an organization must ensure they are implemented securely and in such a way that identities can be trusted.

Internet of Things (IoT)

IoT devices are typically resource-constrained, headless devices. That is to say that an IoT device has limited CPU processing power and memory. Additionally, a headless device is able to act autonomously without a user controlling a device's every action. IoT devices may be stationary or mobile, operating outside the firewall of an enterprise. All of these factors contribute to making an IoT device more difficult to secure than a PC or smart device within an enterprise perimeter. It is essential that IoT devices have a trusted identity. HSMs should be used to protect the root keys used for device identity issuance, onboarding, enrollment/activation, and management. Protecting these keys and integrating an HSM with other processes such as PKI management and certificate management will ensure that the credentials used for authentication and encryption operations are handled securely. HSMs should be used to improve the authentication assurance level at each stage of the IoT device security lifecycle.

Blockchain

A blockchain is a decentralized, distributed ledger technology that maintains a continuously growing list of ordered records called blocks. Each block contains a timestamp and a link to a previous block. Blockchain is used to track transactions such as crypto currencies, financial transactions, and contracts. As a ledger, blockchain does an excellent job of keeping track of records; however, the quality of the information contributed to the blockchain is dependent upon the trustworthiness of the contributors. HSMs can be used to protect the cryptographic keys used for authentication and encryption to ensure the contributor and contributions made to blockchain are trusted.

Quantum

Organizations that are preparing for a post-quantum world require crypto-agility and the ability to integrate quantum random number generation (QRNG) and quantum algorithms into their key distribution (KD) processes. Luna HSMs are designed to integrate quantum technologies as they emerge. In fact, Thales has partnered to integrate QRNG technologies and quantum-safe algorithms into the Luna HSMs to generate the entropy, or randomness, required for quantum-safe security solutions today.

Bring your own key (BYOK)

Companies looking to secure their cloud infrastructure and applications are turning to bring-your-own-key (BYOK) approaches. In this model, organizations create their own keys and securely transfer them to the cloud. Thales has partnered with several cloud service providers, to securely transfer private keys generated by a Luna HSM to a Luna HSMs hosted within the cloud providers data centers.

5G

5G cellular networks will bring low 1ms latency and gigabit throughput to connected mobile devices. 5G will be critical to digitalization efforts that enable automation, M2M connectivity, robotics, rich video streaming, and VR/AR applications. As the telecom industry continues to discuss the overall security model and protocols that will be used to secure 5G communications, companies need to ensure that their devices have trustworthy identities. HSMs should be used to generate and protect the root key used to issue identities to the device. Current 3G and 4G devices often use pre-shared keys (PSK) that can be easily stolen during the provisioning process or when keys are manually changed. HSMs ensure that devices have an immutable identity based on keys that are protected within a FIPS 140-2 Level 3, tamper-resistant vault.

Cloud Native

Cloud native is a term used to describe container-based environments where applications are deployed as microservices running in a dedicated Docker, Kubernetes or LXC container on an elastic infrastructure that is managed using DevOps processes and a continuous delivery workflow. Developing, deploying and running cloud native applications requires security at every step of a continuous integration/continuous deployment (CI/CD) pipeline. Assigning identities to workloads, containers, and devices is critical to enabling other container security solutions to establish secure, encrypted connections between containers. Thales has partnered with a number of cloud native security companies to integrate Luna HSMs into the overall DevSecOps lifecycle.

Connected Vehicles

Connected vehicles require vehicle-to-vehicle (V2V) and vehicle-to-everything (V2X) communications to communicate autonomously with other vehicles and smart city infrastructure such has stoplights, pedestrian walkways, lighting and smart buildings. Electronic control units (ECUs) in cars have digitized the driving experience, and also put more processing power into the vehicle. In order to ensure the trustworthiness of ECUs, device and car manufacturers can use HSMs to generate and store the private keys associated with each ECU. HSMs can also be used to sign code to ensure supply chain provenance of software updates to the car's ECUs and systems.

Secure Manufacturing

More than 85% of connected industrial devices are more than ten years old, making them especially vulnerable to cyber-attacks. Smart and secure manufacturing requires that devices, gateways and networking equipment be protected from inbound and side channel attacks. HSMs can be used to ensure that devices have immutable identities that can be used to effectively authenticate and encrypt data-in-motion and data-at-rest. Trusted identities of system components will also allow industrial operators to ensure the integrity, safety and reliability of systems and the supply chain.

Edge Computing

While cloud computing moved processing to centralized data centers, edge computing is moving computing closer to the end user. Mobile service providers are collocating hyperconverged infrastructure (HCI) and edge servers at cell towers to run cloud native applications across both cloud and edge infrastructure to reduce latency and optimize the performance of applications, such as telemedicine, augmented reality, and gaming. HSMs can be used to protect the keys used in edge computing infrastructure, applications and networks.

Integrations

Luna HSM 3rd party technical integrations help an organization easily and securely implement applications, extending its platform and capitalizing on investments already made, saving time, and improving efficiencies.

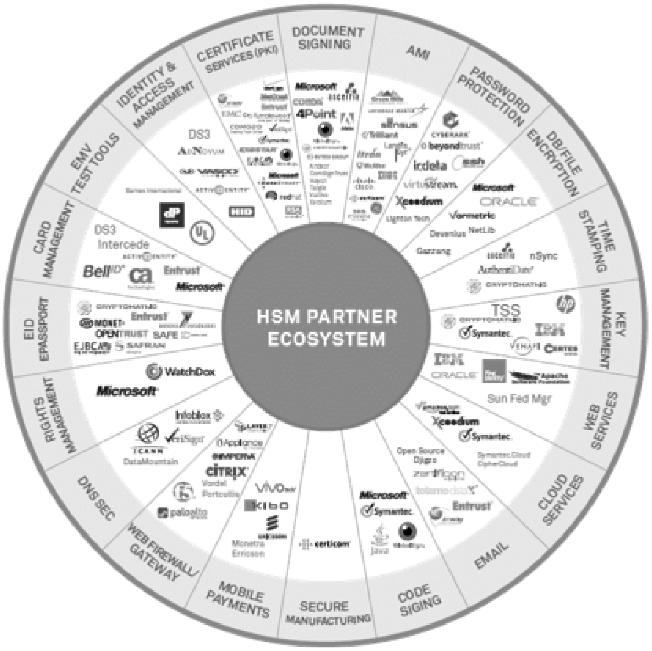

figure 6: Luna HSM Partners

Compliance

Cybersecurity has evolved to a point where minimal acceptable levels of security have become well-defined, and based on these foundations, continue to evolve. Thales is committed to keeping abreast of foundational and evolving compliance recommendations and requirements. The following are examples of how Luna HSMs are addressing cybersecurity compliance standards and requirements where we are committed to providing products and services to meet the growing needs. It is certainly not an exhaustive list, as the cybersecurity needs of our clients grow with each passing day. It is, however, a good overview.

FIPS 140-2 Level 3

The Federal Information Processing Standard (FIPS) 140-2 Level 3 requirement for security products is among the most stringent security hardware requirement globally. Security products designed to these standards must go through rigorous testing and pass both logical and physical attacks aimed at breaking into a secure storage device and obtaining sensitive information, such as security keys. Products designed and certified to the FIPS 140-2 Level 3 standard are required for any US Government secure storage devices, and products designed to the FIPS 140-2 Level 3 standard are the bare minimum any enterprise should use when considering their own secure storage needs. Anything else is frankly a compromise and cannot withstand the rigorous attacks of determined hackers. All Thales HSM products are designed to meet the criteria for FIPS 140-2 Level 3 certification.

Common Criteria EAL4+

Throughout Europe and the rest of the world, including the United States, Common Criteria Evaluation Assurance Level 4 (EAL4) is considered the minimum assurance level for any protection profile attributed to a secure storage device. Luna HSMs are designed to meet the criteria for common protection profiles associated with secure storage devices in order to assure global clients that they are indeed using the highest quality secure storage and encryption devices.

eIDAS

Electronic Identification, Authentication and Trust Services (eIDAS) is a current European Union (EA) regulation requiring, among other requirements, the secure creation of digital signatures by a qualified signature creation device (QSCD). Luna HSMs are not only designed to meet the criteria for a QSCD but have arguably become the gold standard by which other QSCDs are judged.

GDPR

The General Data Protection Regulation (GDPR) is not in full force throughout the European Union (EU). It brings with it very strict requirement for protecting personal data. The fines for failing to comply with GDPR requirements are very crippling, and not only apply to organizations transacting data within the EU, but also to any organization outside of the EU conduction data transactions with EU entities. The fines can be massive, quickly reaching into the millions of dollars for failure to comply. Luna HSMs are designed to provide the foundational data encryption and protection requirements to meet and even exceed the expectations of organizations seeking to ensure both internal and external customers that they are indeed prepared to face the challenges associated with GDPR compliance.

PCI-DSS

The Payment Card Industry Data Security Standard (PCI DSS) was created in the United States in the early part of the 21st century, with the first version being released in 2004. It came about as a result of massive increases in credit card fraud brought about by various factors, not the least of which was the massive increase in credit card transactions. As more payment systems came online it became much more challenging to secure and protect cardholder data. Several members of the payment card industry as well as merchants, financial experts, and security experts formed an alliance to set some fairly rigorous standards for protecting cardholder data. Luna HSMs provide data protection that meets and exceeds PCI DSS requirements. Additionally, Thales is a PCI DSS registered Qualified Security Assessor (QSA) that can provide clients with PCI DSS assessment services and assist them in identifying gaps in their payment card networks and assist in designing them for optimal security performance.

HIPAA HITECH

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 was created to place rigorous standards around health insurers to provide a simplified method of transferring the health data of patients from one provider to any other provider. This came at a time when paper-based systems were quickly being converted to electronic medical records (EMR), with medical data being transferred over the Internet. This led to the creation of the Health Information Technology for Economic and Clinical Health (HITECH) act being enacted and signed into law in 2009. Under the HITECH act organizations are required to protect healthcare data of all patients or face large fines and what amounts to public shaming by the US Federal Government. Patient data must be securely stored at a bare minimum, and it is highly recommended that patient data be encrypted whenever possible. Luna HSMs meet and exceed the requirements for secure data storage under HITECH regulations, enabling healthcare delivery organizations to use EMR systems to improve patient care while ensuring data availability, reliability and privacy.

IEC 62443

IEC 62443 is a group of security standards that have been created to ensure that Control Systems operated in a secure manner. As various parts of the standards have been ratified over the years they have also been presented to ISO for ratification. Besides being accepted as cornerstone foundational security standards for industrial control systems, they have also been recognized as foundational security standards by the FDA as they relate to the security of medical devices.

Among the many security recommendations and requirements found in the IEC 62443 series are the recommendations and requirement for secure data storage, data integrity, and tamper resistance. Luna HSMs enable companies to meet the system requirements for IEC-623443-3-3 and component requirements outlined in IEC 62443-4-2.

SAE/ISO 21434

SAE/ISO 21434 is a current draft standard for vehicle cybersecurity created by the automotive and other associated industries to ensure that network connected vehicles can function in a secure manner. There are thousands of applications, systems, and processes associated with connected vehicles today, requiring the generation and storage of digital keys, certificates, and identities far exceeding in numbers any other digital system ever created. HSMs are critical for securing digital data in back-end systems being deployed globally for vehicles and associated systems and services, as well as for generating the billions of keys and certificates that will be needed as the systems continue to grow.

Conclusion

As organizations modernize their businesses, processes and services with new digital technologies, this transformation continues to usher in new ways of connecting with customers, creating business value, and simplifying the way we work. New technologies such as IoT, blockchain, quantum computing, cloud native and edge computing are creating new security challenges. These new computing models are must be secured by building trusted systems to protect data privacy as well as safe and reliable systems, including applications, devices, network infrastructure and embedded components.

For more than 25 years, Thales has been the market leader with innovative, high-assurance, FIPS 140-2 Level 3-validated Luna HSMs to meet evolving risk and compliance needs. Governments and the most trusted brands in the world rely on Luna HSMs as their foundation of digital trust, protecting the keys associated with PKI, data base encryption, code signing, SSL, cloud, and supporting secure manufacturing, where confidentiality, integrity and availability are paramount. Luna HSMs can also be integrated with emerging technologies such as blockchain, containers, 5G, quantum computing, BYOK, CASB, M2M and IoT, providing crypto agility, reliability, and data ownership in any environment including hybrid and multi-cloud.

Contact us to determine how Luna HSMs can provide your foundation of digital trust across the broad range of technologies that enable your digitalization strategy, ensuring your critical cryptographic keys, digital identities and transactions are always protected.

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 <