thalesgroup.com

THALES

An Anchor of Trust in a Digital World:

Risk Management Strategies for Digital Processes

White Paper

Contents

Introduction

The volume of information is mushrooming and being transformed from paper to digital form at an alarming rate with no end in sight. Individually, we all experience the steady growth in storage capacity and our use of that capacity in the devices we touch daily – our laptops, desktops, and smart phones. On the commercial side, a conversation with the IT data center personnel quickly reveals that adding storage capacity is a perennial budget item.

What should also be recognized is that the value of digitized information is not solely determined by the fact that it exists and its increasing volume, but its use. Business and governmental entities know from experience that the fluidity of digitized information is critical in the advancement of their business operations and citizen-serving endeavors.

The escalating growth in the creation, storage, and use of digitized information also creates a growing exposure of information being lost, stolen, misused, and contaminated. The rise in regulations and laws designed to protect the rights of individuals is tangible evidence that this exposure is real. The rise in incidences of information breaches represents another piece of evidence of this growing exposure.

And it's not just the digitized bits of information associated with individuals that are at risk of exposure when in the hands of business and governmental entities. These entities have their own set of sensitive and valuable information that is at risk when in digitized form, for example: operational information such as business and marketing plans, customer account information, price lists, and financial statements; tactical and strategic plans to protect and serve a citizenry; and various forms of intellectual property.

Considering the growing exposure and potential ramifications of information incidents – such as failed regulatory audits, fines, litigation, breach notification costs, market set-backs, brand injury, and even business failure - business and governmental entities are wise to plan and implement a comprehensive information risk management strategy. A growing number of entities are proactive in this regard and have integrated Hardware Security Modules (HSMs) into their information risk management deployments. In fact, for some entities, HSMs are instrumental in the development of innovative products and services that are only possible through secure storage and use of digitized information.

The purpose of this paper is to introduce Hardware Security Modules and describe the attributes that position HSMs as an attractive component in information risk management.

About the Author

Michael Suby is the Director of Stratecast and an Analyst. In his Director role, Suby oversees the business operations of Stratecast and its research direction. As an Analyst, he contributes to the research themes of Stratecast's Business Communication Services analysis program with a concentration in Secure Networking. Suby's Secure Networking analysis is centered on the technologies, products, and services designed to improve the security of enterprise networks, their business and consumer-facing applications, and sensitive data at rest, in use, and in motion.

Hardware Security Modules

In general, Hardware Security Modules (HSMs) are dedicated systems that physically and logically secure cryptographic keys and cryptographic processing.

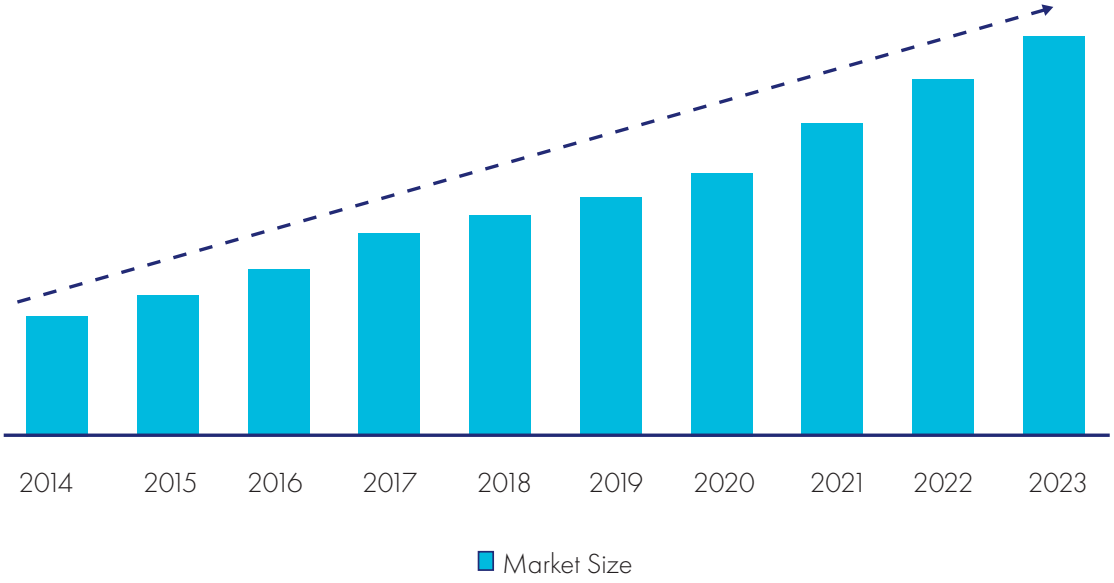
Functions supported by HSMs include:

- Life-cycle management of cryptographic keys used to lock and unlock access to digitized information. Remember that the privacy strength of encrypted information is determined by the sophistication of the encryption algorithm and the security of the cryptographic keys. The most sophisticated encryption algorithm is compromised by weak cryptographic key security. Life-cycle management of cryptographic keys includes generation, distribution, rotation, storage, termination, and archival.
- Cryptographic processing which produces the dual benefits of isolating and offloading cryptographic processing from application servers.

In use since the early 1990's, HSMs are available in two forms:

- Standalone network-attached appliances, and
- Hardware cards that plug into existing network-attached systems.

As the use of encryption to protect the confidentiality of digitized information has increased, partially driven by governmental regulations (e.g., eIDAS (electronic IDentification, Authentication and trust Services) for electronic transactions in the European Market, General Data Protection Regulation (GDPR) for the collection and processing of personal information, and Health Insurance Portability and Accountability Act in the secure transport of heath information over the Internet) and industry mandates (e.g., Payment Card Industry Data Security Standard, Requirements 3 and 4), so too has market demand for HSMs, as shown below.



Corresponding to the increase in market demand for HSMs has been a continuous expansion in HSM features and performance characteristics to address a wider array of use cases. In addition, the comparative differences between HSMs and software-based alternatives have gained clarity. More on these differences follows in the next section.

Hardware Security Modules versus Software

Routinely IT is faced with a decision on whether purpose-built appliances are preferable to software. After all, purpose-built appliances represent another piece of physical hardware for the IT organization to procure, deploy, configure, and maintain. More devices add to the capital expenditure budget, add to overall IT complexity (i.e., more pieces of unique hardware), and perhaps even limit deployment flexibility within the IT environment. With IT organizations already struggling with sizable and diverse hardware inventories and potentially cramped quarters, and keen to reduce their carbon footprints, a "more specialized hardware" approach may not always be the default choice. Software, by contrast, has the advantage of installing and running on potentially existing and dormant servers and can ride the wave of improving server price performance and energy efficiencies. Consequently, software, at least initially from financial, IT operational, and carbon footprint perspectives, appears to be a worthy alternative to purpose-built appliances.

This cursory view of hardware versus software, however, has proven to be less robust when the function in question is security. Most business and governmental entities recognize that security has unique properties that are difficult to rope into the general IT environment while still maintaining functional integrity. As evidence of this, the market for purpose-built security appliances is solidly positive. Where pressure exists to reign in security appliance sprawl, the directions frequently pursued are multi-functional security appliances (e.g., Unified Threat Management appliances) or blade and chassis security platforms. In both instances, security functions remain physically independent from the rest of the IT environment.

HSMs, as previously described, represent a crucial element in protecting digitized information. Attempting to accomplish the same in software should not be done without fully considering the implications. Following is our perspective on this matter.

Completeness

HSMs are fully contained solutions for cryptographic processing, key generation, and key storage. As purpose-built appliances, they automatically include the hardware and firmware (i.e., software) necessary for these functions in an integrated package. Physical and logical protection of the appliance is supported by a tamper resistant/evident shell; and protection from logical threats, depending on the vendor's products, is supported by integrated firewall and intrusion prevention defenses. Some HSM vendors also include integrated support for two-factor authentication. Security certification is typically pursued by HSM vendors and positioned as a product feature.

Software for these same functions is not a complete out-of-the-box solution. Server hardware is a separate purchase, unless unused servers are present, as is firewall, intrusion prevention, and two-factor authentication. Being tamper resistant is not a trait typically associated with general-purpose servers. Security certification encompassing the combination of hardware platform and software would be the responsibility of the user organization and can be a lengthy and very costly activity, especially if involvement with certification bodies is not standard operating practice for the organization using the software.

Performance

Cryptography is a resource intensive process that will introduce latency to any application that depends on it. Depending on the application involved and organization, the objective could be to minimize the latency introduced by cryptography. HSMs have an advantage over software as they are designed to optimize the efficiency of cryptographic processing. Compared to software running on general purpose servers, HSMs will accelerate processing; an outcome of being purpose-built.

Compliant and Secure

Frequently, cryptography is used to meet compliance mandates. Cryptography use, however, does not guarantee that information is secure. Further, there are no security guarantees (i.e., promises of no security instances ever) with any security solution so the objective becomes one of managing risk by reducing the number of vulnerabilities and the likelihood of vulnerabilities being exploited. The aforementioned completeness attributes of HSMs allow organizations that deploy HSMs to take efficient and simultaneous steps toward compliance and security.

Centralization of Key Management

An attribute of software is its portability; software can be installed on several servers. Consequently, cryptographic keys have greater likelihood to reside in several locations/software hosts. This multi-location characteristic will add to administrative complexity and potential lapses in the life-cycle management of cryptographic keys (e.g., rotation and revocation). In addition, if consistency in the protective layer of the software host (e.g., firewall, intrusion prevention, and access control) cannot be ensured, the risk of keys being compromised increases. With HSMs, the tendency is to store keys in a single unit. Not only does this streamline administration and reduce the potential for management lapses but it also supports a consistent layer of key protection.

"According to the European Association of Corporate Treasurers' (CAST) Project, an average cost savings of 80% can be achieved by using electronic invoicing."

- European Electronic Invoicing Final Report

Layered Key Protection

As previously stated, HSMs protect cryptographic keys and that protection is instrumental in ensuring the confidentiality of digitized information. To illustrate the layered approach to protecting keys inherent in HSMs, following are the steps that a key-stealing attacker would need to follow:

1. Gain entrance to the environment where the HSM device has been deployed.

2. Locate and steal the HSM device, which is typically stored in a physically secured safe or locked down in a data center.

3. Disassemble the device without damaging it, including removing the potting material many tamper-resistant HSMs use.

4. Reverse engineer the flash contents of the device to find the key material.

Again, general-purpose servers that host key storage software do not have similar safeguards.

In addition and of equal importance, this same tightly controlled, physically protected environment defends HSM software/firmware from exploits aimed at software vulnerabilities. Without extraordinary and likely cost-prohibitive efforts, defenses on general-purpose servers do not compare.

Back-up and Restore

Operational resiliency is critical to the business pursuits of many enterprises as their clients are intolerant of black-outs and brown-outs in their operations that are tightly dependent on the services of another. If encryption is in the critical path, cryptographic keys must have bullet-proof accessibility and, if not, be immediately recoverable on the heels of a catastrophic event that renders the primary key storage unit inaccessible. Many vendors have designed their HSM devices to support this type of resiliency.

Is a Hardware Security Module always the right approach versus software? Not always as a mix of an HSM and software hosted on general-purpose servers can produce the suitable level of risk management the business or governmental entity seeks and also provide flexibility in deployment and security expenditures. What must remain front and center in a mixed approach, however, is aligning the technical choice of protection with the criticality/sensitivity of information. The more sensitive the information or the more severe the implications of an information breach, the more appealing the attributes of HSMs become.

Trends Increasing Demand for HSMs

The never-ending digitization of information with value, as previously stated, is a primary driver in the use of encryption. As the usage of encryption increases, so too will the need to manage keys at higher levels of efficiency and effectiveness, that is, at an enterprise-grade level. The same is true for cryptographic processing. Fitting, these are the two functional pillars of HSMs.

Other trends that affect how businesses and governments operate in the electronic informational age also spotlight HSMs. Consider the following:

- **Cloud computing.** As organizations continue to test and then integrate cloud computing into their IT environments, HSMs are into service to safeguard cryptographic keys with the same dynamic and virtualized attributes of cloud computing environments. Additionally, when storing data in multi-clouds, using native encryption from cloud service providers creates silos of data and the risk of not having full control over your keys and data. On-premises HSMs diminish those silos and enable users to know the whereabouts of their keys at all times.
- **Cryptography as a service.** At a high level, HSM usage will increasingly be employed to enable a move to the delivery of server-mediated cryptographic services. Rather than simply providing point services to individual infrastructure components, HSMs will become essential infrastructure components, powering cryptographic services upon which a host of applications rely.
- **Evolving data protection applications.** HSMs are increasingly important in powering data protection applications. Today, organizations are deploying access control and encryption technologies to achieve compliance with increasingly higher industry standards—namely FIPS-140 Level 3, Common Criteria EAL 4+, PCI DSS and data privacy regulations. This demand for certification—and the high price of achieving compliance certification internally—drives the increased deployment of HSM technologies in data protection applications.

- **Elliptic curve cryptography.** Elliptic curve cryptography (ECC) provides the same level of security at smaller key sizes than other asymmetric PKI schemes. For example, the degree of security attained with a 2048-bit RSA key can be realized with a 224-bit elliptic curve key, nearly 10 times less in size. The smaller key size of ECC results in reduced requirements for storage, bandwidth, memory, and power; and faster cryptographic operations. These comparative attributes ushered ECC into handheld and wirelessly-connected devices, Internet of Things (IoT) devices for example which have limited storage and processing capabilities but which are more numerous and embedded into electronic operations that involve information of value. Consequently, there is a need for high scalability in key management, a characteristic of HSMs.
- **Post Quantum Crypto Agility.** As most crypto algorithms break over time without warning, and with the post-quantum era just over the horizon, there is an added level of concern. In the quantum era, as soon as a hacker has access to a quantum computer they will be able to weaken today's algorithms by breaking them or reducing the strength of the symmetric crypto keys and crypto hashes. Practicing crypto agility enables you to quickly react to cryptographic threats by implementing alternative methods of encryption. HSMs protect and manage encryption keys and enable the update of cryptographic algorithms in the field, providing the crypto agility to quickly react to cryptography threats and implement alternative methods of encryption.
- **Blockchain**. Although blockchain's decentralized and distributed digital ledger brings many benefits, its entire premise rests on the integrity of the blockchain. HSMs decrypt digital keys and provide high assurance protection of blockchain ledgers and digital wallets without compromising efficiency.

Conclusion

In order to address current and emerging compliance mandates, as well as the increased threat of devastating security breaches, business and governmental entities around the world, across a multitude of industries, have employed HSMs. HSMs provide organizations with the unrivaled security benefits of a hardware boundary that delivers physical and logical protection that software alone simply cannot match. Further, by offering centralized key storage, scalable cryptographic processing, and robust security mechanisms surrounding backup and restore, HSMs significantly streamline security administration. As businesses and governments seek to leverage these proven strengths, security architects will only grow more reliant upon HSMs—both to guard against evolving threats and to capitalize on the emerging opportunities posed by technological advances. To assist in these efforts, it will be incumbent upon HSM vendors to rise to the challenge of supporting such initiatives as cloud computing, enterprise key management, cryptography as a service, the post-quantum era, IoT and more.

"Using an HSM for online PIN issuance is a perfect example of how we strive to make banking secure and convenient for our customers. We are constantly seeking to adapt our products and services such that they fit in with their modern lifestyles."

—Head of Architecture and Innovation, Consumer Bank

Annex

HSM Use Cases

To prevent these data breaches from occurring, leading enterprises and government agencies have been turning to HSMs in order to protect sensitive data and applications at their source. For instance, organizations in the financial service industry, one of the largest targets for cyber thieves' attacks, have been at the forefront of using HSMs to secure their digital processes. HSMs are used in a variety of applications, such as securing cardholder and PIN processing and issuance, transaction authentication, paper to digital security initiatives, as well as data confidentiality and cryptographic key management. Following, are some detailed examples of the various ways HSMs are used in financial services and a host of other industries.

IoT Medical Device Code Signing

A large medical device manufacturer was launching a next generation medical device that relied on blue-tooth technology. Requirements included the need to secure its next generation Internet of Things (IoT) device, quick time to market, and the need to meet strict compliance regulations. This organization relied on HSMs to provide critical continuous security; IoT medical device compliance; a secure PKI anchored by the on-premises HSM; signed code updates; and quick time to market. Furthermore, it was able to ensure tight controls for easy auditing.

Cloud Security and Complete Key Control for Financial

A well respected financial institution was migrating to IBM's cloud infrastructure. A mission-critical requirement was that the Bank, and only the Bank, maintain control of their encryption keys and ultimately their data. The deployment of a Luna HSM together with a key manager provided a high-assurance data protection solution, ensuring that the financial institution always had the utmost control over their data, security policies, and the keys that protect that data regardless of whether that data was hosted in the IBM Cloud or on-premises. The Enterprise was able to leverage a hybrid model with a hardware root of trust and vault the master keys in its on-premises data center.

Online Credit Card PIN Issuance

A large online bank was looking to roll out an entirely new way of payment for its customers—enabling them to use a payment card with an embedded chip and a PIN to verify their identities rather than having to sign a printed receipt.

Using postal mail to distribute PINs was insecure, costly, and slow, so they decided to leverage the Web as a new PIN delivery mechanism but needed a solution that was highly secure and cost effective to deliver and manage the PIN. The bank used an application security module that featured an integrated FIPS 140-2 Level 3-validated HSM. With this approach, the bank was able to ensure that cryptographic keys and processes were stored and managed exclusively within FIPS-validated hardware. Code signing and verification were used to maintain the integrity of the Java application code and prevent unauthorized application execution. Additionally, strictly enforced access and usage policies would prevent unauthorized access to sensitive applications or data. With tamper-resistant hardware, network connectivity, and secure remote administration, the HSM made it possible for the bank to deploy sealed high-assurance Java Web service applications, which proved to be a project-enabling capability.

The employment of HSMs, and the use of a secure online process, eliminated the huge exposure of sending out PIN information in the mail. Additionally, the bank realized significant cost savings: For every million-card customers, the bank saved hundreds of thousands of pounds in postage and fulfillment costs while providing the customer with better service. Plus, as opposed to the mailing of PIN requests, which can take up to ten days, online PIN requests could be fulfilled instantly, which means customers could use their cards more quickly—and the bank could start seeing revenues faster.

Electronic Invoicing

Across the globe, numerous compliance mandates, such as the Brazil Nota Fiscal (NF-e) and the European Directive on Invoicing, have emerged to place security requirements around the practice of electronic invoicing. The European Directive on Invoicing (EC/115/2001) requires member states to implement electronic invoicing into their local value-added tax (VAT) legislation to improve and streamline cross-border invoicing. The VAT rules require suppliers to guarantee the following:

- Authenticity of origin, meaning that the message content was actually created by the person or legal entity that signed it.
- Integrity of invoice content, ensuring that no changes have been made to the invoices during transit.

In order to comply with the VAT law, the port authority for a major European city implemented an advanced e-invoice solution based on digital signatures. The port authority leveraged its investment in Adobe's LiveCycle Enterprise Suite (ES) and GlobalSign's DocumentSign digital certificates by selecting an HSM that offered easy integration with these applications.

The organization used HSMs to store digital signatures and protect cryptographic keys. The integrity of both cryptographic keys and digital certificates are vital to the integrity of the overall security system—if the keys or digital certificates were compromised, the entire system is rendered obsolete.

After Adobe LiveCycle ES converts an invoice into a PDF/A (Archive)-compliant document, digital signatures are applied using a digital certificate to ensure the authenticity and integrity of the PDF. The PDF invoices are digitally signed with a secure private signing key, which requires an HSM capable of performing certificate authority management tasks. The HSM stores the keys within the secure confines of the appliance throughout the key life cycle.

The HSM enables the organization to secure digitally-certified invoices and to cryptographically bind the identity of the certifying party to the invoice. The Adobe PDF Reader automatically verifies all of the embedded information, and visually highlights the authenticity and integrity of the document, allowing the recipient to easily detect whether the document has been altered after being certified. By applying digital signature and encryption technologies within a PKI network environment, the firm quickly brought digital invoicing processes online, thereby streamlining workflow, lowering costs, and meeting mandatory European directives for compliance.

Check Imaging

In the move from paper check filing to digital management of check images, a large bank needed to implement a host of safeguards to ensure the integrity and security of these digital files. HSMs were used by the bank to sign and verify digital check images, offering protection against erroneous and unauthorized check payments.

By moving to a digital check imaging system, the large bank also recognized quicker check processing times. Now, once a check is deposited with a bank, it is almost always delivered overnight to the paying bank and debited from the check writer's account the next business day.

Securing Financial Transactions and Communications

A bank sought a way to secure financial transactions, communications, and digital identities. Existing MPLS networks did not adequately secure transfers between the bank and other regional banks. Additionally, there was no way to secure and manage the identities of the system users in order to create reliable and secure non-repudiation characteristics.

The firm deployed a complete PKI infrastructure using Microsoft Certificate Authority, HSMs, and a time stamping authority. This infrastructure enabled the bank to issue certificates to system users for authentication and signing. In addition, it secured communications between local banks by signing and encrypting financial transactions, payments, and email communications.

This new deployment enabled the bank to launch a new service for local inter-bank transactions that was more cost-effective compared to other alternatives, and provided for secure communications between banks. The bank is now able to digitally sign any type of transaction—both quickly and securely.

Online Buyer Authentication

To reduce online fraud and increase consumer confidence in online shopping, Visa and MasterCard introduced authenticated payment programs known as "Verified by Visa" and MasterCard SecureCode. Specifically, Verified by Visa (VbV) employs 3-D Secure, which adds a step to the checkout process to verify the identity of the cardholder. During the checkout process, the 3-D Secure system requests that the card-issuing bank verify the online user as the legitimate cardholder.

As part of this initiative, an issuing bank that participated in the Visa program employed an authentication system to verify the identity of the payer during online transactions, and they had to ensure this system complied with VbV security standards. An underlying challenge of the system was to secure the generation, storage, and management of the cryptographic keys used by the encryption, digital signature, and cardholder validation processes that form the building blocks of the VbV system.

If attackers were to capture these critical keys, the authentication system would be exposed to exploits that could seriously undermine the system's security and erode consumer brand confidence. Because of this threat, the card associations defined stringent measures for key protection. They mandated that the cryptographic keys securing messages between the cardholder, merchant, and card issuing banks during the 3-D secure verification process, must be stored within a FIPS 140-2-validated HSM.

The issuing bank's HSM ensured that sensitive cryptographic keys or processes were never exposed to potential attackers, where they could be stolen or manipulated to create fraudulent authorization of illegitimate transactions. The HSM selected features dedicated hardware cryptographic processing, complete hardware-based key life cycle management, and a proven three-layer operational, software, and physical security model. The HSM also supports the high availability configuration needed to support this mission-critical environment.

Through an exchange of encrypted and digitally-signed messages between the merchant's software, the Visa Directory, and the software's VbV Access Control Server, the cardholder is authenticated and the transaction is processed. HSMs provide the trusted signing devices required for the series of messages and routines that are performed to authenticate the transaction and comply with VbV standards.

By using a robust HSM, the issuing bank was able to ensure that all messages and routines used to validate and authenticate payments are secured via tamper-resistant hardware, ensuring the highest level of integrity for online transactions. In addition, the issuing bank satisfied its need to demonstrate adherence with best practices through the use of FIPS-validated hardware.

E-Passports

In their efforts to boost border security, and better guard against identity theft, illegal immigration, and trans-border crime, governments have been integrating smart chips into passports. In addition, these technologies promise to help reduce the time it takes for individuals to make it through the screening process at border crossings.

To ensure data authenticity and integrity, the information in the chip has to be digitally signed by the respective issuing authority. When the electronic passport holder reaches an immigration entry desk, the immigration officer verifies the personal information and biometric identifier stored in the chip.

The trust of the digital signature is bound to the security of the corresponding digital signing key. Many countries around the world have been employing HSMs, both at the location in which passports are initially issued and at locations in which passports are inspected, such as border control offices. In these cases, HSMs are used for secure key generation and storage, digital signatures, encryption, and encoding the passport holder's personal data on the smart card chip.

Biometric Security

The U.S. Transportation Security Administration's (TSA) Registered Traveler Program allows for certain individuals to have their identities verified using biometric technology, so, once identified, they can take advantage of expedited screening at participating airports.

A vendor participating in the Registered Traveler program needed to secure their root CA and central information management system (CIMS), both to protect the identities of users and to ensure the integrity of the TSA's system. The vendor used an HSM to ensure the confidentiality, integrity, and non-repudiation of sensitive cryptographic keys. Their HSM received FIPS 140-2, Level 3, and Common Criteria EAL4+ certification, and offered support for two-factor authentication and multi-level access control. In order to provide the most robust security, HSMs were used to secure other critical cryptographic keys, including the subordinate certificate authorities, XML, SSL encryption keys, and other application-specific keys.

The firm configured network-attached HSMs in a cluster in order to ensure high availability, meet defined service level agreements and performance requirements, and achieve long term scalability. They were also able to seamlessly integrate their HSMs with Microsoft Certificate Services, and provide Java, C, and CAPI API's for custom application development.

Secure Manufacturing

In order to guard against forgery, many manufacturers are turning to HSMs to protect their intellectual property, such as chips, hard drives, printer components, amongst others; as well as protect against lost revenue. One such manufacturer wanted to protect their phones used to do snooping, identity forgery, and other forms of network abuse that plague the cellular phone and satellite television industries. This IP phone manufacturer needed to integrate secure identification and authentication into its devices. The business needed to integrate the issuance of digital identities and authentication into its manufacturing processes, which meant the organization would need to securely and cost-effectively create thousands of industry compliant digital identities.

The IP telephone manufacturer selected Microsoft Certificate Services software for managing the issuance of the digital identities, but needed a hardware solution to deliver maximum security and performance. A highly secure hardware system was required to protect the certificate issuance root key—the basis of trust for all of the IDs issued to the phones—and prevent the possibility of a copy of that key being used to create illegitimate device identities. The solution also had to meet high performance standards to ensure that the computationally-intensive certificate issuance process did not create bottlenecks in the manufacturing process.

The manufacturer selected an HSM as the foundation for their digital identity issuance system for IP telephones. Their selected HSM received both FIPS 140-2 and Common Criteria certification. With each IP telephone containing a unique, trusted digital identity, users can be sure that the IP telephone they are connecting with is definitely the telephone it claims to be. This IP telephone manufacturer's use of HSMs demonstrates how high-volume, high-speed digital ID issuance can be seamlessly integrated into the manufacturing process without sacrificing security.

Process Controls

A large software vendor sought to implement a process control solution that required the use of digital signatures to approve software code and other deliverables as they moved from one stage in the workflow to the next. For this vendor, the process control solution was very large scale, comprising several thousand different approval chains and tens of thousands of private keys—each one unique to a particular stage in one of the approval chains.

The development team started to implement its process solution in software and realized part way through the implementation that the overall administrative complexity was becoming unmanageable. Ultimately, the group decided to abandon the in-house development effort and, instead, started to look for a cryptographic module that could help simplify the implementation.

Once they had selected and deployed an HSM that fit their situation, the development effort, which had been bogged down by the complexity of securing key storage and cryptographic processing, was much more efficient. With the HSM in place, the development team could focus on the work flow and process control logic, while treating cryptography like a simple utility.

The integration of the HSMs went smoothly, allowing the implementation team to get the project back on schedule, which ultimately enabled the organization to realize its process control objectives in a timely manner. In addition, a few years after the initial HSM deployment, the company's software development focus shifted from Perl to Java. Because the organization's HSMs supported standard APIs, including the Java cryptographic API, integrating the HSMs into the new development environment was a relatively simple matter.

Web-based Application Services

A global financial services company wanted to deploy an extensive, Web-based environment for delivering application services. Initially used within their internal network, the firm ultimately planned to deliver these services to customers.

Over time, the organization's system incorporated hundreds of network-attached HSMs, securing a wide range of keys and associated on-line services—including Web server SSL/TLS private keys and certificates, keys used to secure Web services applications, and private signature keys used to authorize transactions.

Many of the HSMs' inherent capabilities were critical to ensuring the ultimate success of the initiative. The HSMs offered support for high availability, load balancing, and remote management—including the ability to manage keys at even the most remote sites—which were all crucial features for the organization.

Security Appliance Certification

A security appliance vendor was challenged with ensuring certification and regulatory compliance of its products. Establishing and maintaining compliance represented a large upfront and ongoing cost for the organization. Subsequently, the vendor embedded a third-party HSM, which had all the requisite certifications. By leveraging a commercial HSM within the product, the vendor's development organization was able to focus on the core solution offering, and still meet industry regulation and compliance mandates—all while reducing ongoing certification expense.

THALES

Americas
Arboretum Plaza II, 9442 Capital of Texas Highway North,
Suite 100, Austin, TX 78759 USA
Tel: +1 888 343 5773 or +1 512 257 3900
Fax: +1 954 888 6211 | E-mail: sales@thalesesec.com

Asia Pacific – Thales Transport & Security (HK) Ltd
Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East
Wanchai, Hong Kong | Tel: +852 2815 8633
Fax: +852 2815 8141 | E-mail: apacsales.cpl@thalesgroup.com

Europe, Middle East, Africa
350 Longwater Ave, Green Park,
Reading, Berkshire, UK RG2 6GF
Tel: +44 (0)1844 201800 | Fax: +44 (0)1844 208550
E-mail: emea.sales@thales-esecurity.com

> thalesgroup.com <