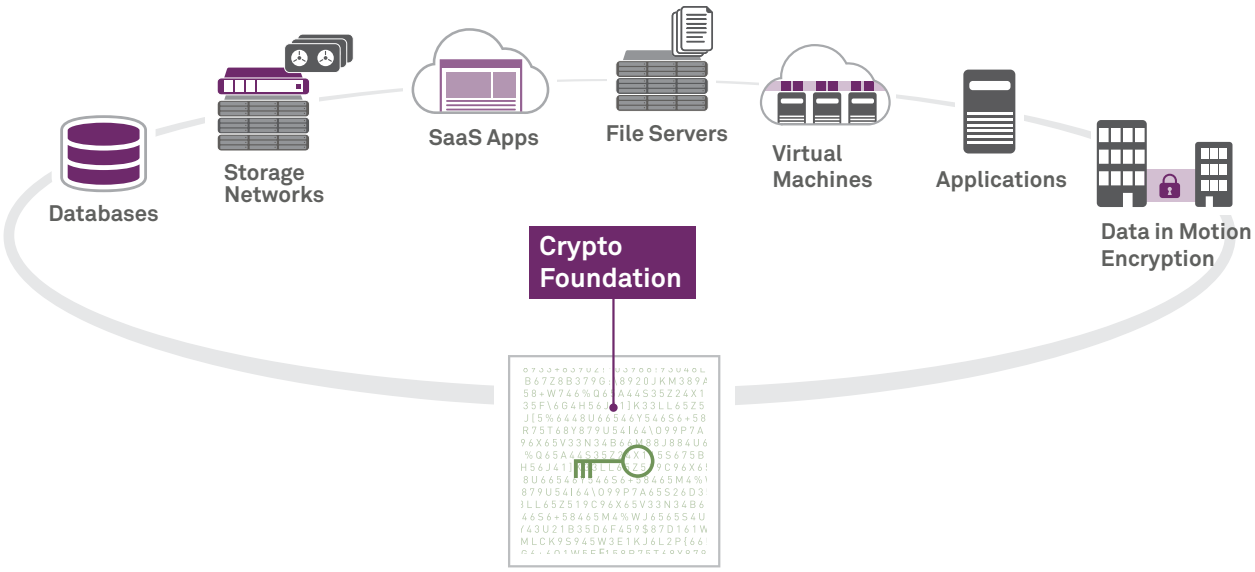
gemalto
security to be free

Everything you need to know about
Crypto Management

Contents

The New Data Security Landscape

The proliferation of cloud applications, mobile devices and virtualization has created many shared environments and an unlimited number of end points, leaving data incredibly vulnerable. Escalating threats compounded by expanding regulatory requirements is altering the data security landscape. The best way to secure sensitive information is by placing safeguards around the data itself through encryption. As the use of encryption becomes more widespread and diverse, many organizations are realizing they need to adopt a strategy that centralizes these accumulated 'encryption islands' and allows them to migrate to the cloud. It's a fair assumption that new types of threats will emerge leading to new types of encryption within new places. This is why organizations need to take the time to vet any weaknesses within their environment and implement a 360 degree data protection plan that covers all bases now and in the future.



Encryption

Whether you are reassessing your current security infrastructure or putting one in place for the first time, encryption should be approached in the same way an organization establishes a security policy.

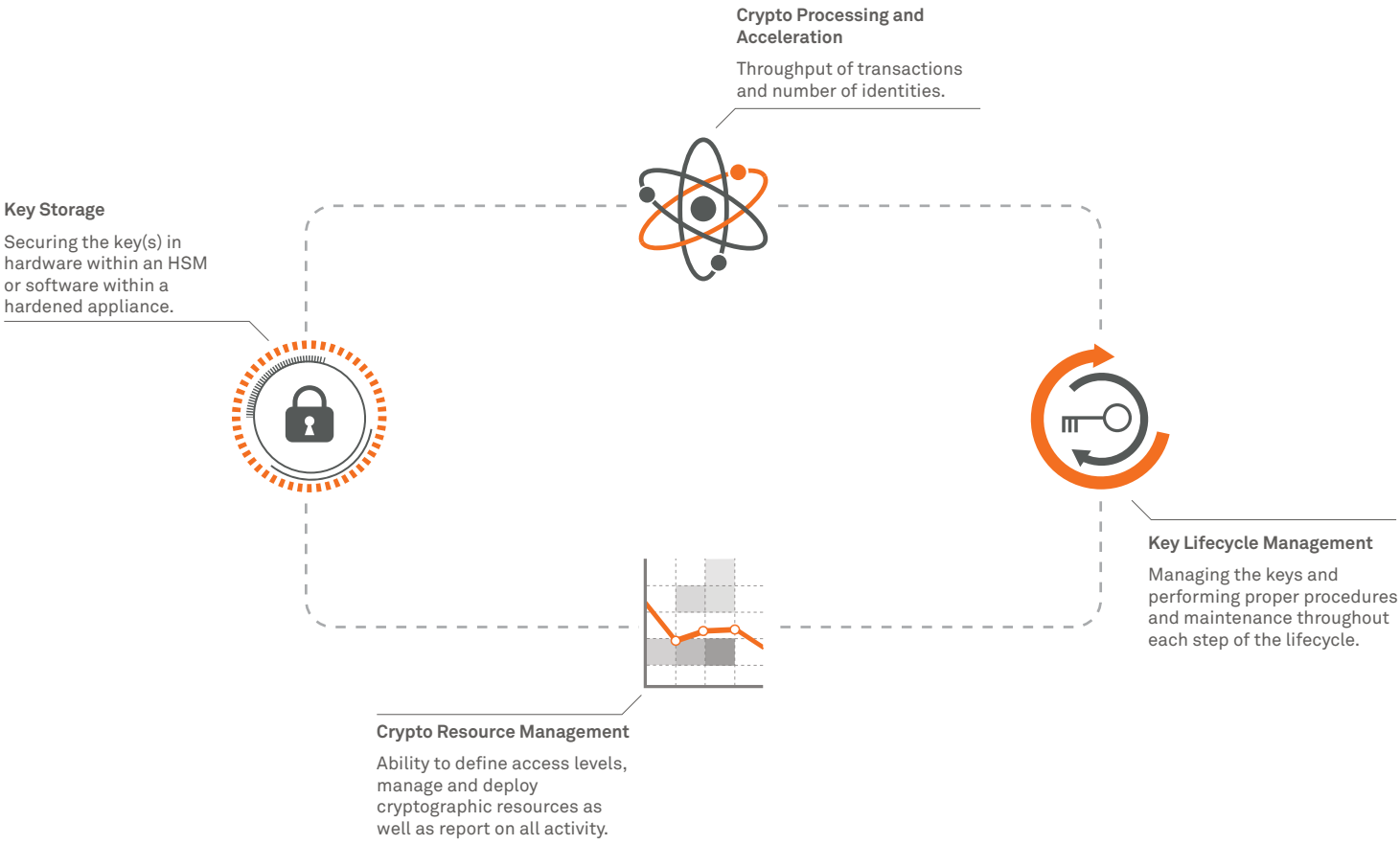
- Detect your threats and locate all sensitive information. First, conduct a risk assessment of the business in order to understand what types of data are present, where the data is stored and the flows or patterns of the data.
- Determine the level of encryption required: data in use (such as databases containing customer information, data at rest (financial information in file servers, and back-up in storage networks) and data in transit as it crosses the network to/from your public/private cloud computing environment. You must consider all of the various threats that apply to data at different points within the lifecycle and then select the best encryption solution based on requirements and that given set of data.

What About the Cryptographic Keys?

Aside from implementing a strong method of encryption, it's crucial that your encryption keys are treated with the same level of circumspection. Once data is encrypted, the only way to gain access again is by decrypting or unlocking secret content using the key. Haphazardly protecting these keys negates the entire process of encryption and creates a false sense of security. Therefore, the security deployment should utilize best practices for both encryption, as well as key management—creating a Crypto Foundation.

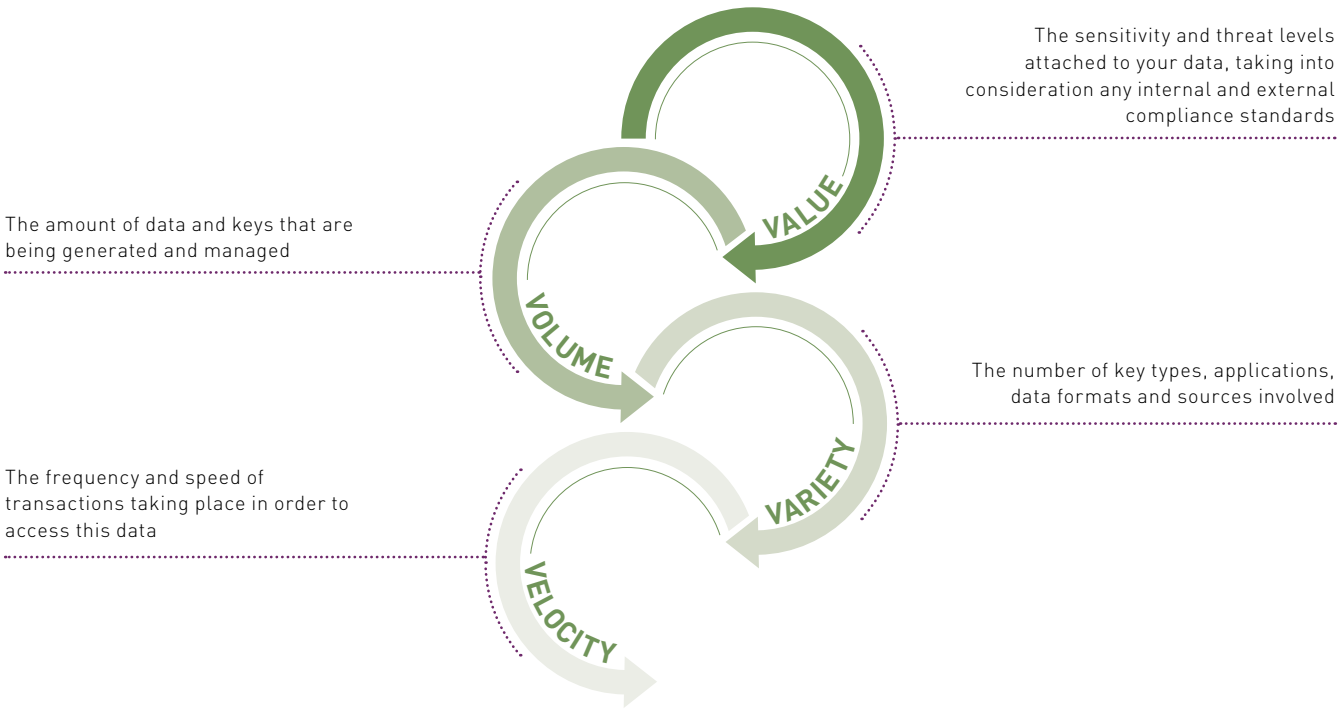
Building a Crypto Foundation

A Crypto Foundation is a centralized approach taken to secure various types of data in different environments, combined with the management and maintenance of keys and crypto resources being utilized. In order to provide the consolidation, protection and flexibility that today's business environment demands, a data protection strategy should incorporate the following four key areas:



Once these areas are factored into the strategy, organizations no longer have to rely on the bare minimum procedures established by their application vendors. They are free to build, maintain and manage each area according to their specific use case(s). The concentration levels of each will depend on existing infrastructure, compliance mandates, and the Four V's.

The Four V's Model



Value

- Are your crypto keys trusted?
- Is the origin of your keys secure?
- Where are your keys?
- How are your keys protected (hardware or software)?
- Would your keys pass an audit?
- Does FIPS, Common Criteria, PCI, PII matter to you?

Velocity

- Does crypto operation speed matter?
- Does Key Generation speed matter to you?
- Are you performing crypto transactions on small or large data packets?
- Which Crypto operational performance matters to you? (Sign/Verify, Encryption/Decryption, Key Generation)

Variety

- What are your High Availability needs?
- What are your disaster recovery needs?
- Are you delivering keys to distributed end points?
- Are your encryption use cases growing?
- Are you managing "islands of encryption?"
- Is consolidating your encryption infrastructure a challenge today?
- Is consolidating governance and compliance a challenge today?
- Do you have internal and/or external audit and compliance needs?

Volume

- How many keys do you need to generate and manage?
- Does your answer on volume vary based on different use cases?

1. Crypto processing & acceleration

Take stock of the types of information you are currently encrypting or need to incorporate in order to achieve your goals. Ensure that cipher/algorithms are comparable with current industry standards and widely used, as the classification of 'strong' cryptographic algorithms can change over time. You may want to consider elliptic curve cryptography which allows you to make really strong keys that take up very little memory. Next, establish key lengths with the right combination of protection and flexibility. Compliance mandates can help guide best practices to follow.

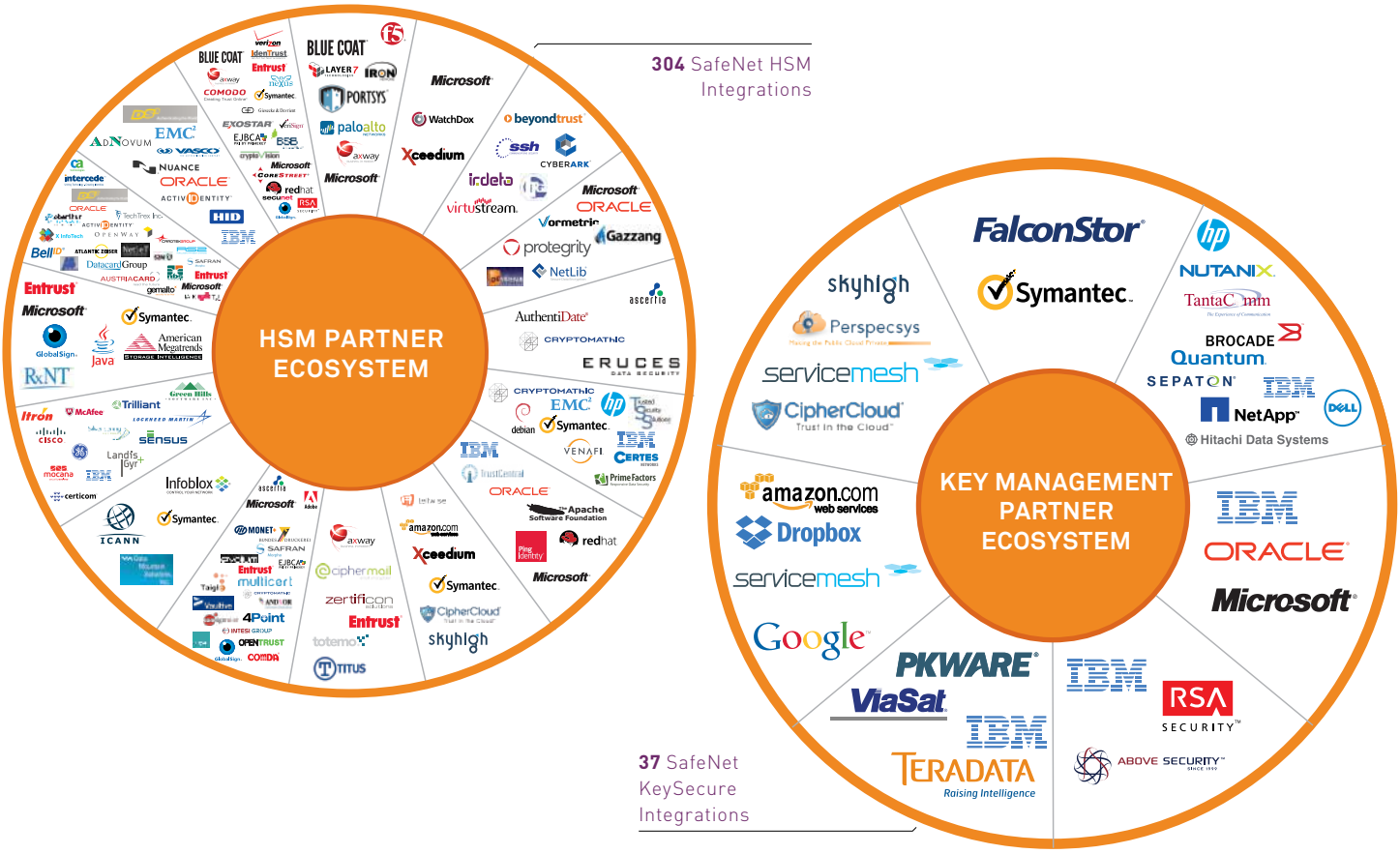
Look at current workflows and applications. Where will encryption and decryption take place? Depending on where you want encryption to run, and the velocity, you may need to consider incorporating high-speed cryptographic processors. Appropriate offloading and accelerating crypto operations will help to avoid processing bottlenecks and increase system capacity. Intelligent load balancing ensures uninterrupted operation and highest availability.

Hardware security modules (HSMs) can provide a solution for offloading cryptographic processes from application servers to dedicated hardware. An HSM is a specialized computing device that performs cryptographic operations and includes security features to protect keys and objects within a secure hardware boundary, separate from any attached host computer or network device. Storing the keys in hardware also provides an additional layer of security for the cryptographic deployment.

The key is to find a solution that can be easily implemented and supports industry standard APIs out of the box, which can greatly simplify integration. Having the flexibility in performance, scalability, usability, and security will ensure your crypto foundation is able to support both business and security goals.

> An HSM is a specialized computing device that performs cryptographic operations and includes security features to protect keys and objects within a secure hardware boundary, separate from any attached host computer or network device

Gemalto Integration Ecosystem



2. Key storage

The proliferation of encryption in today's enterprise has created a situation where keys are stored in inconsistent states of security. Protection of cryptographic keys throughout their operational life is essential to the security of all encryption systems. Systems may use different types of keys including symmetric and asymmetric keys. Some rely on a root key and a certificate, creating a trust link where keys involved are symmetrical or identical for both encrypting and decrypting a message. A more hybrid solution may rely on distinct, asymmetric key pairs using a working session key. Session keys live momentarily and are the last thing to encrypt, but the root key is the constant in the system and has to be the most secure.

The requirements of your use case(s) and environment will determine the keys' roles and ultimately how they are stored. Depending on the value of data being protected, and the variety of keys needing to be stored, organizations have the option of storing their keys within hardware or software. For keys that are trusted to protect highly sensitive data and applications, a centralized, hardware-based approach to key storage is recommended.

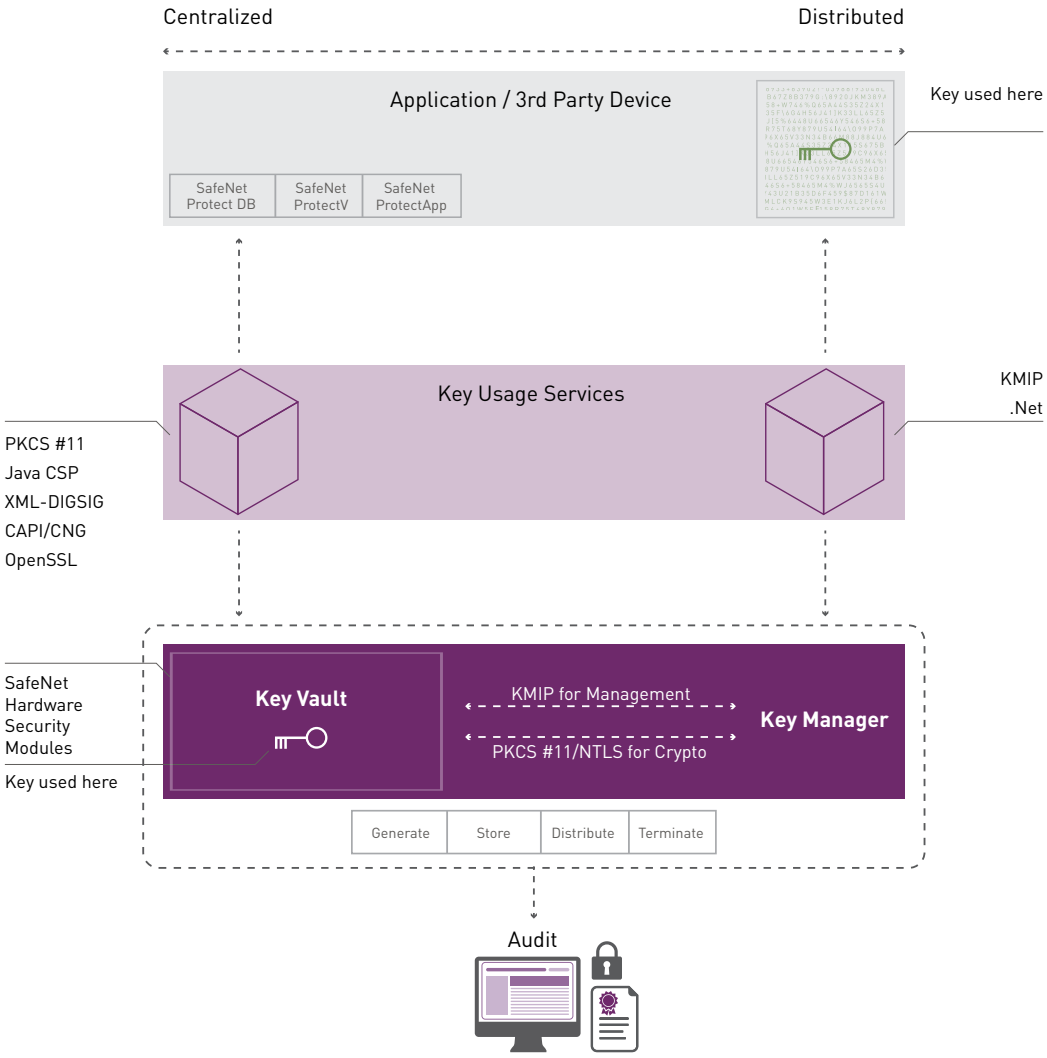
Centralized key storage (keys stored in hardware)

The highest assurance model when it comes to the security of your data is to store the key(s) within a hardware security module. Nothing ever enters or leaves the tamper-resistant vault so keys are more isolated from traditional network attacks and should the HSM become compromised, the keys will zero out. This approach is required by several compliance mandates: The National Institute of Standards and Technology's Federal Information Processing Standard (FIPs-x) and The Common Criteria for Information Technology Security Evaluation. These certifications indicate that the appliance has been through stringent third-party testing against publically documented standards.

Placing a gap between the threat vectors that have access to your data and the threat vectors that have access to the keys is best practice. Use cases, such as code signing, certificate validation, transaction processing and Public Key Infrastructure, involving a limited number of applications are an ideal fit for the centralized key storage model, which requires limited key distribution, used for one specific reason.

Some applications will require a more distributed model, where cryptographic keys must exist in close proximity to the data and applications they secure.

Centralized vs Distributed Key Management



Distributed key storage (keys stored at the endpoints)

Organizations trying to encrypt mass amounts of smaller segments of data, requiring high availability and usage may gravitate toward this model. For instance, data within customer databases usually requires a lot of keys moving across many applications. Keys are called upon to encrypt sensitive data and store it within applications as needed. Vast amounts of keys are required to accommodate seemingly unlimited transactions, and these keys are kept in proximity to the database for efficiency and convenience.

It's important to note that the security of the underlying master keys can impact the trust placed in thousands of distributed keys. Where possible, organizations are encouraged to generate keys using a highly secure master key stored in an HSM.

These keys can then be wrapped, using algorithms designed to encapsulate cryptographic key material, and distributed to endpoints as needed. This allows companies to maintain a high volume of keys and transactions necessary to conduct business while still ensuring all keys are protected to the utmost.

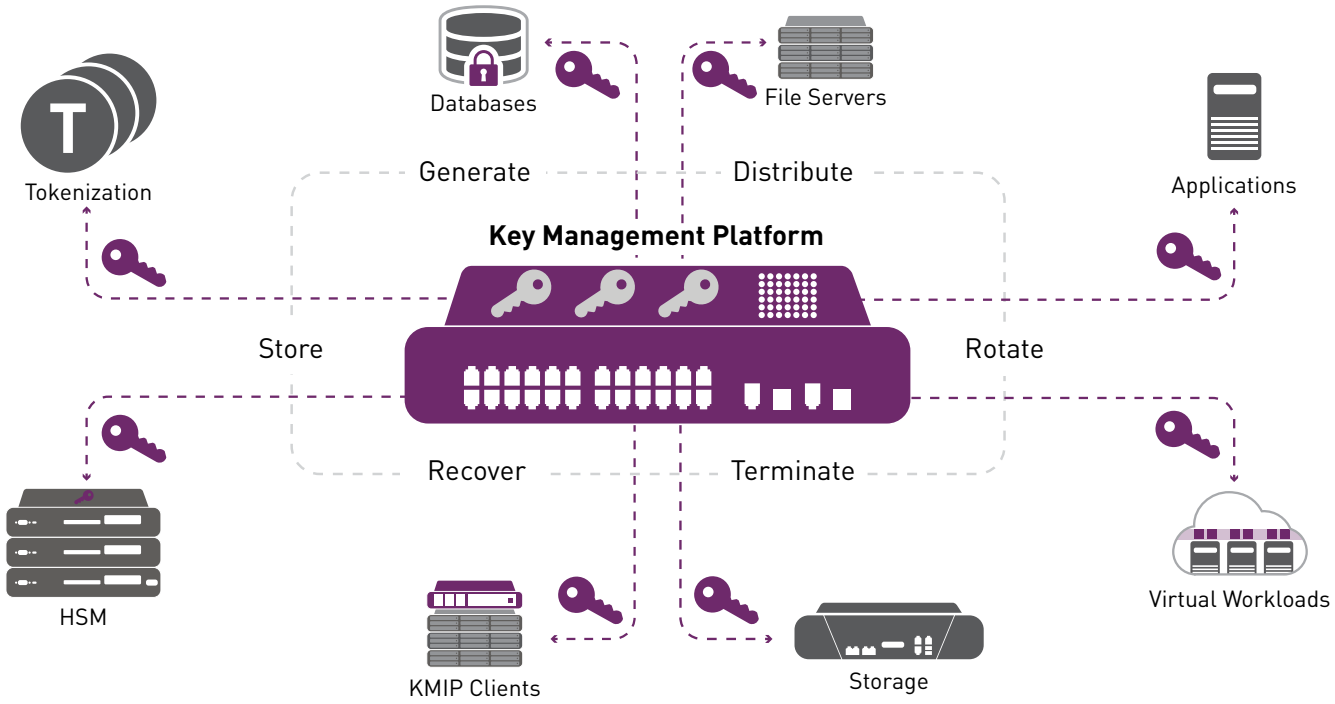
Effective key management should also be used to alleviate some of the vulnerabilities of keys stored in a distributed fashion.

3. Key Lifecycle Management

Successful key management might arguably be the most challenging aspect of building a crypto foundation, as it involves an integrated approach around generating, storing, distributing, rotating, revoking, suspending and terminating keys for devices and applications. More than likely, various encryption solutions have been deployed and accounting for all of those affiliated keys and disjointed systems becomes unsustainable. The stakes are high and mismanagement of keys could lead to exposed data.

Effective key management is particularly needed when keys are stored in the distributed model. An organization warranting high volume, velocity and variety of keys, might consider investing in a system that specializes exclusively on key management duties. This centralized management platform will perform all key-related tasks and tie back to other systems or HSMs that are performing cryptographic operations using those keys.

Understanding the various key lifecycle states is important to properly plan key management requirements:



Key generation and certification

Since a key is used to encrypt and decrypt vital data, make sure the key strength matches the sensitivity of the data. In general, the length of the key coupled with how randomly unpredictable keys are produced are the main factors to consider in this area. The greater the key length, the stronger the encryption. The strength of the key is essential to the mitigation of the threat of brute force attacks.

Enterprise-wide encryption policies should also be established. Security administrators should define a standard set of criteria and mandate a standard set of tools to meet the requirements wherever encryption is required.

Key distribution

Before being distributed, a key must be associated with a particular user, system, application or policy. The association will determine the requirements to secure the key, and ultimately the method used to secure it while in transit. The type of cryptography used will determine the appropriate method of key distribution. In symmetric key cryptography, secret keys must be securely exchanged between parties. Wrapping these keys prior to distribution can provide security as they travel through otherwise unsecure networks. In public key cryptography, private keys must be stored securely, while public keys may be widely distributed without fear of data loss.

Lastly, the ability to differentiate access between the administrator creating the key and the person using it is vital. By having this separation of duties, business owners can rest assured that they have minimal risk of unauthorized users getting access to confidential information.

Key storage

For keys that are trusted to protect highly sensitive data and applications, a centralized, hardware-based approach to key storage is recommended. Some applications will require a more distributed model where cryptographic keys must exist in close proximity to the data and applications they secure.

Key rotation

Depending on the algorithm and organizational need, each key should be designated a crypto period with the ability to change that key on demand. It's important to limit the amount of data encrypted with a single key because using the same key over a long duration of time increases the chances that the key will be compromised. Furthermore, it can be impossible to tell when keys are lost, stolen or copied, so rotating keys regularly ensures stolen keys are only useful for a specific time period. Once rotated with a new key, the existing data should be rekeyed. Rekeying is the process of decrypting data and re-encrypting it with a new key in order to protect it from any undetected compromise of older keys.

Key back-up and recovery

If the key storage mechanism fails or is compromised, there must be a way to restore the keys. Otherwise, the data is encrypted and lost forever. Backup copies of cryptographic keys should be kept in a storage mechanism that is at least as secure as the original store, so keys can be restored and data decrypted and re-encrypted with a new key. Ideally, using an offline storage container, such as a FIPS validated card, appliance or token is best practice. Be sure to document concrete procedures to handle a key compromise as well.

Key revocation, suspension, termination

Every organization needs the ability to revoke, destroy or take keys offline. In the event of a compromise, an organization can delete the keys associated with the compromised systems or data and by doing so, ensure unauthorized users will never get the keys required to decrypt sensitive assets. Depending on the circumstance, there may be the need to take a key out of the lineup but not terminate it. For instance, data subject for litigation will need to be recalled upon and therefore should only be suspended.

4. Crypto Resource Management

In order to ensure consistent policy enforcement, provide transparency, and maintain the health of your system, every organization should have one, easy-to-use interface to administer, monitor and provision all cryptographic resources.

Deploy resources

Provision and de-provision cryptographic resources for HSMs, automate client provisioning based off partitioning capabilities and create multi-tenant, tiered security administrator access levels. Organizations have multiple stakeholders, which take part in the key management lifecycle. Control of the cryptographic keys should be established so that System Administrators and Security Officers can perform their duties without compromising the Application Owner duties of access and control over the keys.

Configure policy

Determine how many keys can be generated, and where they are stored. Continue to update variables in the system, such as back-up networks and users. Establish a policy for key usage, defining application and device access levels and to what extent they can perform. For instance, only users who are highly trusted and trained to perform key custodian duties should be able to recover the key in case of a loss.

Monitor and report

Secure, automated and unified logging and reporting are absolutely crucial to maintain requisite risk and compliance posture. Key ownership must also be clearly defined, and all modifications recorded and securely stored in order to provide an authentic and trusted audit trail of key state changes.

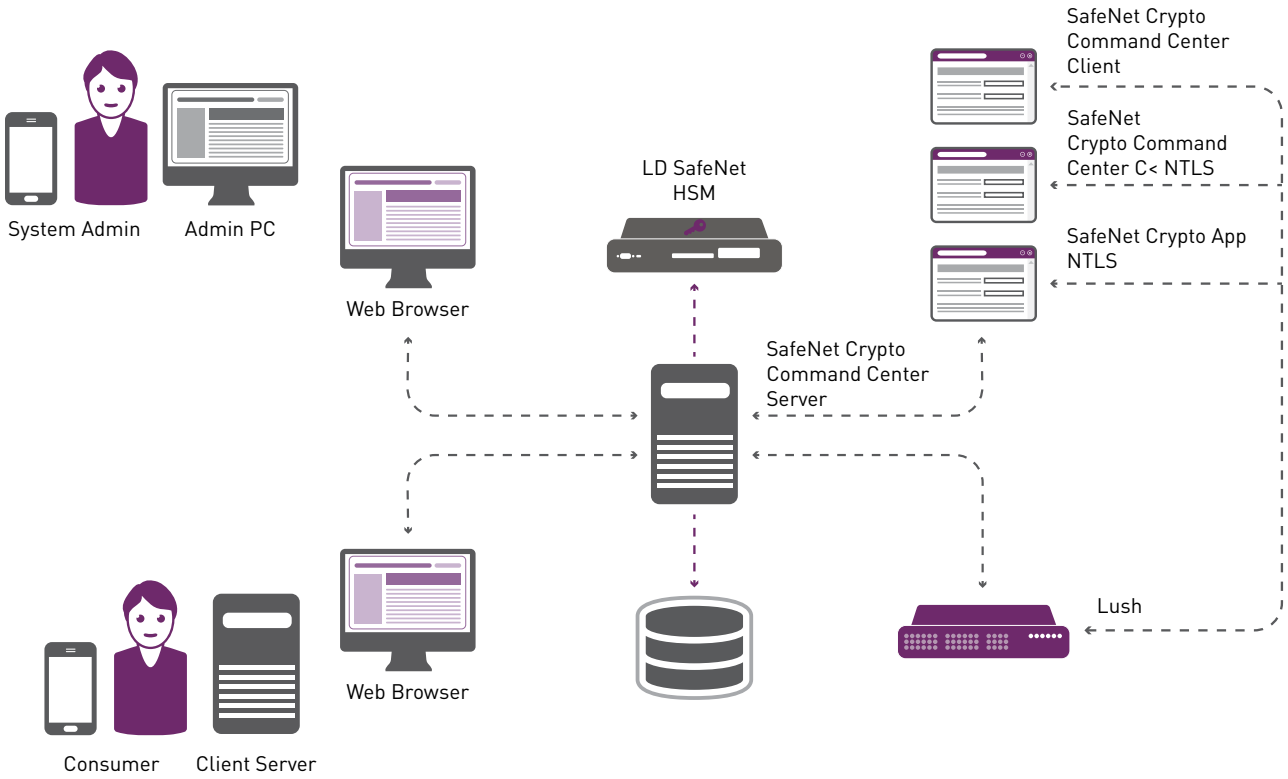
- Proper monitoring indicates how keys are being used as well as identifies failures in the cryptographic devices and unmanaged end-points.
- Reporting capabilities securely track and store audit trails to be signed for non-repudiation. Automated reports and email alerts may be set-up based on a number of cryptographic management criteria.

By leveraging a cohesive, centrally managed platform, IT and security teams can become much more nimble in adapting to changing requirements and challenges. New encryption services can be rolled out quickly and effectively, and data is free to move throughout the enterprise to support business objectives, without compromising security.

SafeNet Crypto Command Center changes the paradigm of how cryptographic resources are deployed by introducing a method for provisioning legacy platforms, such as hardware security modules (HSMs), in a way that fits the cloud model.

With SafeNet Crypto Command Center, security administrators can create a centralized pool of high assurance cryptographic resources that can be provisioned out to the people and lines of business in their organization that need them. Administrators set up a catalog of predefined and configured hardware security modules, and place them in a catalog of items. Using these catalogs, end users can select the resource they need and spin up that resource when they need it. It's on-demand self-service like the HSM world has never seen.

Crypto Command Center Provisioning Components



Cloud Security

Cloud Enablement and Data Center Consolidation

Cloud computing is fundamentally transforming the way enterprises, government agencies, and small businesses are managing their data and their infrastructure. It provides a number of benefits such as lower costs and faster deployment, but it also brings challenges related to data control, security and visibility. The lack of physical control, or defined entrance and egress points, bring a whole host of security issues – data co-mingling, privileged user abuse, snapshots and backups, data deletion, data leakage, geographic regulatory requirements, and cloud super-admins, to name just a few. So how can organizations safely migrate over to cloud and virtual environments?

The Role of Encryption and Key Management

Encryption is the answer to cloud security. As indicated by the Cloud Security Alliance, strong encryption with key management is one of the core mechanisms that cloud computing systems should use to protect data, control data, and ultimately—maintain compliance. However, in most cases, current systems are preventing the move to the cloud. Most organizations have implemented encryption solutions on an 'as needed' basis and have done so without a clear over-arching strategy. Now they are faced with trying to manage disparate, isolated islands of encryption scattered across workgroups, infrastructure and other locations. This leads to thousands of keys residing in inconsistent levels and states of security, creating tremendous challenges in the auditing process and leaving detrimental gaps in security. Who has had access to keys, have these keys been fully maintained, who maintains lawful key ownership?

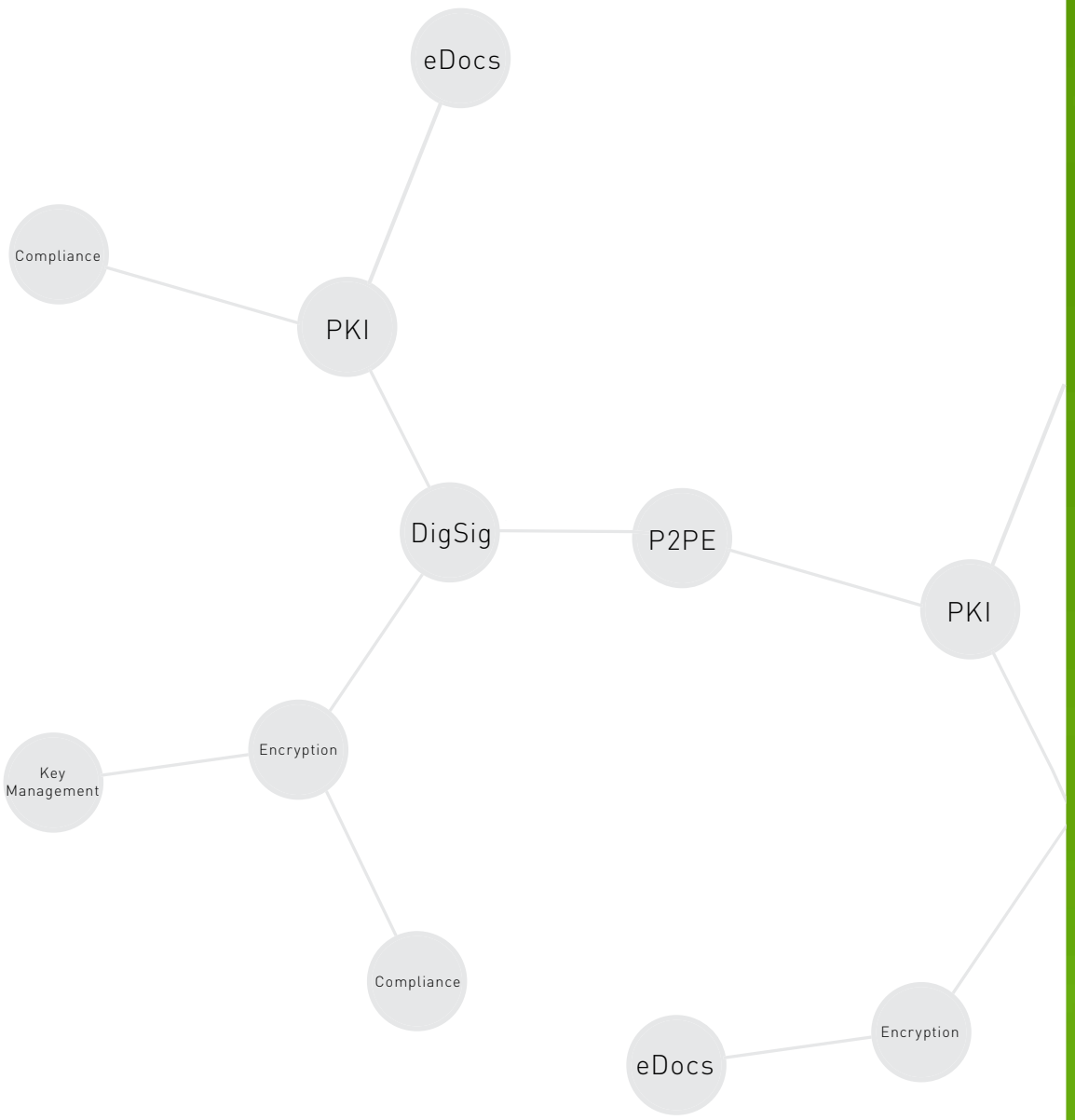
When it comes to rolling out cloud encryption and key management, organizations are most concerned with the following:

- Loss of control of cryptographic keys – Keys are the new target when it comes to breaches, so protecting those keys is paramount! Organizations must maintain key ownership even if they are using a cloud provider. By tap-proofing your keys, you can ensure that government officials and third parties must come to you for the master key.
- Adherence with compliance mandates – Staying compliant has a whole new set of complexities in the cloud.
- Difficulty in auditing system – Software-based deployment can be harder to track.
- Fear of system downtime – Most will have to place their trust in a cloud vendor.

Projecting Key Management in the Cloud Delivery Model

On-demand self-service – users can get the encryption services they need without the intervention of a service provider or administrator
Rapid elasticity – encryption resources can be increased or reduced depending on need
Measured service – encryption usage is monitored, controlled and reported for transparency
Broad network access – resources are accessible from a wide range of devices and locations
Resource pooling – resources are pooled to accommodate multiple customers/lines of business
Key Management for point solutions – keys and policy centrally managed by a standardized management protocol (KMIP)
Provisioning resources - a way to provision out resources, while still maintaining separation of key material using different partitions - then deliver those allocated resources to applications, workloads, line of business and customers

Use Cases


eDocs
Compliance
PKI
DigSig
P2PE
PKI
Encryption
Key Management
Compliance
Encryption
eDocs

Electronic Documentation (eDocuments) Overview

eDocuments, including eInvoicing, eProcurement, eMortgages, eContracts, etc. have become commonplace in today's society. However, trust remains a critical requirement for the feasibility of eDocuments. Digital signatures, powered by encryption and public key infrastructure (PKI), represent the means for establishing trust in eDocuments. Digital signatures give all parties the confidence required to trust that documents come from known entities, they have not been altered in transit, and provide a means for non-repudiation. In turn, these digital signatures need to have foolproof, comprehensive security mechanisms to protect them: If digital signatures are in any way compromised, the entire chain of trust in the eDocument infrastructure will be at jeopardy.

Compliance

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.

Use Case

Antwerp Port Authority manages Europe's second largest shipping port, managing more than 16,000 ships and 65,000 barges each year. In order to comply with the VAT law, the Port Authority 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.

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.

Requirements for solution

- Comply with the VAT law
- Store digital signatures
- Protect cryptographic keys
- Offloading cryptographic processing from application servers
- Easily integrates with existing applications

The Benefits of eDocuments with HSMs

Enhance Security and Ensure Compliance

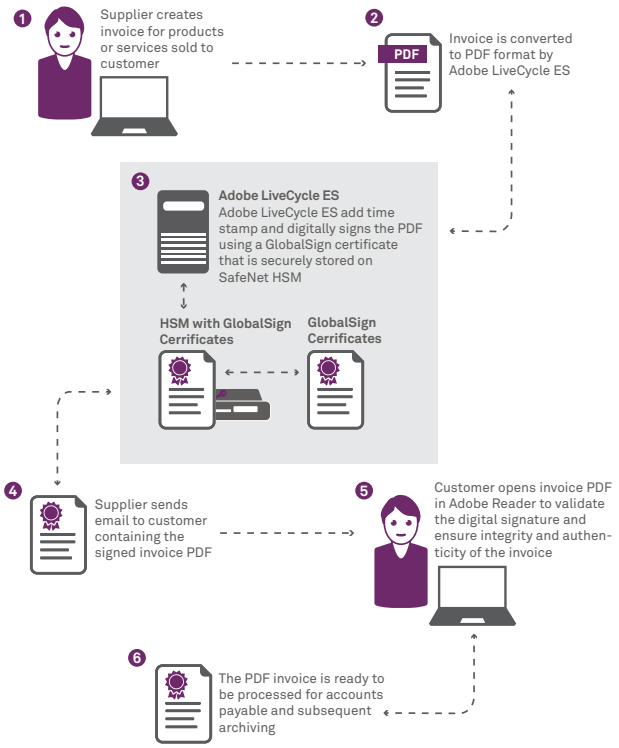
- Certification
- Compliance
- Multiple signatures

Optimize Operational Performance

- Efficient retrieval, processing
- Elimination of time consuming, inefficient paper-based processes
- Improve vendor relations
- Reduced errors, reconciliation times
- Efficiency through back office integration

Reduced Costs

- Centralized keys and policy management



Point to Point Encryption Overview

Recent breaches in the retail sector have necessitated the use of encryption to protect cardholder data. Point-to-point encryption (P2PE) is a means of encrypting credit card data from the point of interaction, such as a card reader, and maintaining the card data in an encrypted state until it arrives in the payment solution provider's secure decryption environment. To remain competitive, payment application providers have started creating their own P2PE solutions.

Compliance

P2PE solutions are growing in popularity because they provide a highly secure method of protecting transaction data, and reduces the scope of PCI-DSS compliance for customers. P2PE solutions must be approved by the PCI Security Standards Council (PCI SSC), and are required to use a hardware security module for key security.

Use Case

As a provider of multichannel payments to large corporate organizations in Europe, The Logic Group needed to deploy a PCI P2PE-compliant solution that could provide its customers with robust encryption, decryption, and key management. The organization ultimately developed Solve DataShield, a P2PE offering that was delivered as part of the organization's secure payment solution. Solve DataShield features a secure PIN Entry Device (PED) that is deployed at the store. When deployed, the PED immediately encrypts the cardholder information submitted. That encrypted data is ultimately sent to the merchant's PCI-DSS-compliant datacenter, or if they are using a managed payment service, the compliant datacenter of the service provider. From there, the transaction is authorized and routed immediately to the acquiring bank for settlement.

In architecting the solution, the service provider needed to implement HSMs within their managed payment service infrastructure, so they could address P2PE requirements surrounding the environment in which encryption and decryption of card holder data would occur.

By leveraging a commercial HSM, the organization was able to quickly and cost-effectively implement a solution that complied with P2PE standards, and well as the following benefits:

- Increased security and reduced risk: By leveraging The Logic Group's Solve DataShield offering, merchants are able to eliminate the holding of customer credit card data in store, which strengthens security and reduces the risk of data theft or compromise.
- Enhanced consumer trust: By reducing the risk of a data breach with a robust security platform, organizations can foster increased trust among their customers.
- Reduced audit costs: With the Solve DataShield solution, merchants can completely remove their stores from the scope of PCI DSS audits, significantly reducing the associated efforts and costs.
- Streamlined administration: Customers can dramatically reduce the time and effort internal teams have to dedicate to security administration by adopting a complete solution.
- The P2PE standard provides detailed requirements that outline how to protect data as soon as it is collected from a chip-and-PIN device until the payment settlement process is complete and includes a number of requirements relating to the hardware used for encryption, decryption, and key management.

Requirements for solution

- Compliant with FIPS 140-2 Level 3 standards
- Capabilities for generating PINs and cryptographic keys
- Scalability to support high-volume transaction environments
- High availability, load balancing, and secure key backup

Benefits of P2PE using an HSM

Offers support for a range of electronic funds transfer (EFT) and payment system processing environments

- Delivers card issuance and transaction processing security functionality
- Provides support for both HSM and host-stored keys
- Enables secure printing of PIN mailers, without risking the exposure of PIN verification keys
- Offers support for the fast and efficient migration of key materials

Regulatory Compliance of Sensitive Data Overview

The number of regulations and mandates has increased over the past few years, as has the scope, complexity and cost of complying with new and existing mandates. The guidelines, rules, and interpretations of each regulation continue to evolve, as do the infrastructures and assets that need to be protected—and the risks they're exposed to. Compliance has become such an immense challenge that organizations can easily allocate up to half of their IT staff to compliance efforts alone, including interpreting vague legal language, implementing solutions for unique requirements, monitoring and responding to regulation updates, meeting compliance deadlines, and managing different audit reporting requirements. In this environment, the traditional approach of treating different compliance regulations as distinct projects, and implementing them in isolation from other compliance mandates creates duplicate efforts, and drives up the cost and complexity of becoming and staying compliant.

Many organizations have turned to data encryption to achieve compliance with multiple mandates, enforcing policies by denying access to sensitive data unless the person or entity possesses the proper encryption key. However, the traditional, multiple-point approach to encryption creates islands of security with disparate encryption systems, key management, and reporting – further exacerbating complexity and cost of compliance.

To eliminate vulnerabilities and gaps in security, forward-thinking organizations are moving away from traditional approaches and towards solutions with integrated encryption, key management, and reporting platforms. It is important for these solutions to have end-to-end encryption platforms with central key and policy management, enabling reporting across databases, applications, file servers, networks, and endpoint devices. This allows companies to implement a framework-based compliance approach with a common platform, where the same standardized technology is deployed throughout the organization.

Use Case

A European insurance broker works with leading Insurance companies and has processed more than 10 million health records -containing personally identifiable information, patient records, health data like sick leave, maternity leave and any other risk related to occupational injury or death within the local government entities. Due to the confidentiality of the records they process, protecting that data is a top Board-level management and organizational priority.

The organization's security department was given the remit to find a cost effective, secure solution that would both increase the level of security of the sensitive data being processed through the company's internal databases, but also complied with local data protection laws and regulations for protecting this data.

In close collaboration with the legal department, business line areas, and other business services, the security team identified the best solution to:

- Increase the security level of the data processed in the internal databases of the organization
- Be in compliance with existing regulations (Basel ll Convention Belorgey)
- Constitute the most cost-efficient, cost-effective solution

By selecting a centralized key manager for their database encryption requirements, the insurance company was able to encrypt all the data stored in the databases so that information is only visible by authorized users. The encryption reinforces the security which, until then, was only based on access control via an application. The distinction between exclusive rights to access data by another way than through the applications, and the exclusive rights to access the encryption and de-encryption keys enabled the company to strengthen the security of data.

Requirements for solution

- Implement a comprehensive risk management framework and standardize on a common set of IT controls
- Reduce system complexity and automate previously implemented manual controls
- Centralized key management via LDAP or Active directory
- Enable encryption without affecting existing infrastructure and applications
- Easily encrypt data with no data loss
- Ability to encrypt data in order to comply with legal and regulatory requirements, while being transparent to users
- Keep within a low budget with no additional in-house development costs

Benefits for framework-based compliance approach using a key management platform

- Secure Ownership of Data throughout its lifecycle, wherever it resides.
- Increased operational efficiency and productivity by encrypting and decrypting information transparently, without disrupting business operations, IT performance, or end-user experience.
- Simple administration
- Met compliance regulations at reduced costs

Enterprise Key Management Overview

As organizations implement encryption on various databases, storage systems, applications, or virtual and cloud deployments, many have relied on native encryption for that technology, or chosen solutions ad hoc based on the project's requirements. The result is an organization with various islands of security, all managed and audited individually. This mishmash of disparate encryption solutions not only requires additional personnel to manage, but makes it virtually impossible to enforce corporate security policies, or repurpose existing technology to accommodate ever-changing best practices, regulations and mandates.

Furthermore, with native or ad hoc solutions, encryption keys are typically stored in software. Many best practices, and even industry and government regulations, are now requiring keys to be stored in hardened appliances, often with FIPS certification.

Use Case

As a government agency responsible for domestic security, the Austrian Federal Ministry of the Interior (BM.I) wanted to ensure that confidential information could only be read by authorized personnel. At the same time, they needed a solution that streamlined administration, and fit into their modest, taxpayer-funded budget.

The infrastructure and operations group sought out an encryption and key management solution that would secure sensitive data, seamlessly integrate with their existing storage technology, and enforce a new "four-eyes" policy that enables granular permission assignments, and requires at least two people to approve permission changes, limiting the number of people accessing data and the power of security administrators.

By selecting a Key Management Interoperability Protocol (KMIP)-based key management solution, the agency was able to seamlessly integrate key management into its existing architecture. KMIP protocols enable one key management solution to pull encryption keys from all KMIP-based encryption platforms into one central management console, thereby consolidating administration responsibilities and enabling organization-wide policy enforcement. Automated operations further streamline security administration - for example rotating keys on a regular basis, generating audit reports and signed access logs – freeing IT staff to focus on more critical projects.

LDAP and Active Directory integration enable the BM.I to assign individual employees' data access using existing user profiles, and easily change or revoke that user's permissions, as well as log all activities, ensuring confidential information remains secure and accessed only by authorized personnel.

Requirements for solution

- Centralize key management via LDAP or Active directory
- Separate duties between data access and security administration
- Enforce corporate security policies
- Centralize auditing and logging
- Easily integrate with existing applications
- Store encryption keys in hardware or hardened virtual appliance

Benefits of Enterprise Key Management with a hardened appliance (KMIP compatibility)

- Manages encryption keys from any technology built on KMIP protocols
- Overlays on existing storage, datacenter, application, cloud or VM encryption solution

Enforce corporate policies and enable compliance

- Manages key lifecycle - key generation, rotation, storage and backup, distribution, deactivation and deletion
- Eliminates time-consuming and inefficient key management processes for individual encryption solutions
- Enables separation of duties
- Controls individuals' access to data via LDAP and Active Directory
- Digitally "shreds" data by deleting encryption keys

Reduced costs

- Simplifies auditing, reporting, and logging with one centralized management consule
- Centralized management reduces time dedicated to key management on disparate systems
- Automated operations further frees personnel to focus on mission-critical projects

FIPS 140-2 Level 3 validation

- Stores keys in hardware appliance with integrated PCI card
- Enables compliance

Gemalto offers one of the most complete portfolios of digital security solutions in the world, enabling its customers to enjoy industryleading protection of identities, transactions, payments and data – from the edge to the core. Gemalto's portfolio of SafeNet Identity and Data Protection solutions enable enterprises across many verticals, including major financial institutions and governments, to take a data-centric approach to security by utilizing innovative encryption methods, best-in-class crypto management techniques, and strong authentication and identity management solutions to protect what matters, where it matters. These security solutions combined with state-of-the-art data generation and issuance solutions and the intrinsic robustness of our certified EMV-compliant range of products, guarantee the optimal security of customer data and payment credentials throughout their entire lifecycle. With all of these solutions, Gemalto helps organizations achieve compliance with stringent data privacy regulations and ensure that sensitive corporate assets, customer information, and digital transactions are safe from exposure and manipulation in order to protect customer trust in an increasingly digital world.

Contact Us: For all office locations and contact information, please visit safenet.gemalto.com
Follow Us: blog.gemalto.com/security

GEMALTO.COM

gemalto
security to be free