gemalto
security to be free

WHITE PAPER

Why Centralized Key Management Is Critical For Scalable Enterprise Storage Security

Executive Summary

Over the last few years, as the requirements for data confidentiality and privacy have been magnified, encryption of stored data in the enterprise has become a much more compelling value proposition. In turn, many discrete storage encryption solutions, along with their customized key management systems, have been, and continue to be, implemented.

Eventually, however, there is an uncomfortable realization by the respective organizations that the resulting key management challenges of comprehensively maintaining and managing all these disparate "encryption islands", further exacerbated by the rapidly expanding number of affiliated cryptographic keys, has become increasingly unsustainable.

The need for a centralized Enterprise Key Management (EKM) system that can interoperate with a wide assortment of existing, and future, storage encryption contexts, and scale to accommodate the organization's evolving security and compliance demands, is clear.

In this paper, the current storage encryption and key management landscape will be examined, the fallout that has accompanied the swift expansion of these separate and divergent systems will be identified, and the core attributes and requirements for a centralized EKM system will be presented.

> "A central key management server provides consistent enterprise-wide security policy execution, including archiving and scheduled updates of keys. Today, nearly all such enterprise key management systems are proprietary."
>
> Excerpt from "SNIA Storage Security and Best Practices"

Introduction - The Existing Storage Encryption Landscape

The Spread of Multiple Heterogeneous Storage Encryption Solutions – And The Resulting Proliferation of Keys

Over the last few years, there has been a dramatic increase in both the market acceptance and deployment of encrypted storage solutions implemented in Direct-Attached Storage (DAS), in Network Attached Storage (NAS), within Storage Area Networks (SAN), and in Tape Libraries. There have been several drivers for this, including organizations' need to comply with regulatory mandates, to increase the protection profile of their critical intellectual property assets, and to avoid costly and reputationally damaging publicly disclosed data breaches.

These hardware and software storage encryption solutions may exist in the form of Full Disk Encryption (FDE) as a Serial Attached SCSI (SAS) device, as Self-Encrypting Drives (SEDs) in a SAN disk array, on a Fiber Channel switch, as encrypted files or partitions in a NAS filer, as encrypting tape drives in a Tape Library archiving solution, or in several other possible formats.

Each of these autonomous encrypted storage solutions is then bundled with its own vendor-specific, often product-specific, and most often proprietary, key management system. This fragmented approach can start organically within an organization, with a single implementation of a selected vendor's product based on a particular departmental or business unit requirement. But it can quickly expand to multiple systems that then require extensive and ongoing manually-intensive operations in order to provide the organization with any kind of wholesale view of the vital key management activities that are essential for uninterrupted data availability, obligatory reporting and auditing functionality, business continuity, and operational risk management.

This piecemeal method has several undesirable consequences. Left unaddressed, it eventually leaves IT security managers with an unenviable challenge of growing

these key management systems to accommodate expanding infrastructure workloads and the resulting explosive propagation of encryption keys. And the problems just continue to amplify as the interoperability chasms dividing all these individual key management systems become ever deeper and wider.

With All Those Expanding "Encryption Islands" – Key Management Has Become a Nightmare

The cumulative effect is a collection of disjointed key management systems, each with its own policies, processes, tools, and staff training requirements. At a minimum, this disparity nearly assures considerable manual intervention, which can dramatically alter the organization's risk posture. Without a centralized view of the involved key management systems and key states, lack of visibility could easily lead to additional, unnecessary, and unwanted business risks due to the organization's inability to holistically monitor key management activities and measure their alignment with its associated Key Performance Indicators (KPIs). It also escalates the very real potential for encryption keys being compromised or unavailable, which could result in unauthorized and material information disclosure or loss. Other unattractive repercussions often include the following:

- **Consolidated logging and reporting efforts become large, unwieldy, manual, labor-intensive projects.** In this type of divergent environment, necessary cyclical efforts to assemble the required all-inclusive logging and reporting involving these key management systems eventually become extensive and costly undertakings. For sound risk management, and to satisfy related regulatory mandates, automated, consolidated and aligned key management policy guidelines, key state monitoring, and secure audit logging and reporting are indispensable.
- **Increased (often substantially increased) operational costs for the organization.** Putting a precise price tag on what this disconnected key management environment costs an enterprise over time encompasses many variables. Although exact quantification varies, operational costs are almost guaranteed to rise, perhaps substantially, due to the lack of federated key management automation and consequential demand for manual "discovery and assembly". Additionally, the potential for lost data records due to unrecoverable or compromised keys, and those correlated operational costs, continue to rise. Add to this the heightened risk of a publicly known security breach – possibly involving customers' personally identifiable information – and the exposure costs could suddenly escalate exponentially.
- **Accelerated deployment of encryption storage solutions increases difficulty to conform to risk management and regulatory compliance mandates.** For the majority of enterprises, relevant regulatory mandates have broadened over the past few years – and the pertinent guidelines, rules, and interpretations for affected stored "data-at-rest" continue to evolve. In response, many organizations have installed a range of storage encryption solutions in the hope that they will strengthen their overall compliance posture, and to more optimally manage their operational risk.

> "Compliance is the main driver for encrypting data-at-rest."
>
> Independent Study by Ponemon Institute - Sponsored by Trusted Computing Group

As the following quote from a study sponsored by the Trusted Computing Group illustrates, regulatory compliance mandates are the primary motivation for encrypted storage implementations:

"According to 51 percent IT practitioners, the main reason to encrypt data-at-rest is to comply with state or federal data protection laws followed by 49 percent who say their organization complies with self-regulatory programs such as PCI DSS, ISO, NIST and others. The state laws include the California Security Breach Notification Act, the recent Massachusetts and Nevada data privacy security and encryption laws as well as other state privacy laws. At the federal level, there are regulations such as the Health Insurance Portability and Accountability Act (HIPAA), including the Health Information Technology for Economic & Clinical Health Act (HITECH)." Excerpt from Independent Study by Ponemon Institute - Sponsored by Trusted Computing Group – May 2011

However, as more storage encryption systems are positioned to address these compliance-related challenges, there are quite often nagging, unintended consequences. Ironically, the compounding system and key management inconsistencies could actually result in overall deployment deceleration, or even contraction.

Effectively Addressing the Encryption Islands Problem

Obviously, all these disassociated storage encryption systems present major challenges with respect to ongoing maintenance, management, and auditability. To provide scalability, deal with regulatory compliance requirements, and to maintain an organizationally-appropriate operational risk posture, an automated centralized EKM system is fundamental to interoperable and cohesive storage encryption.

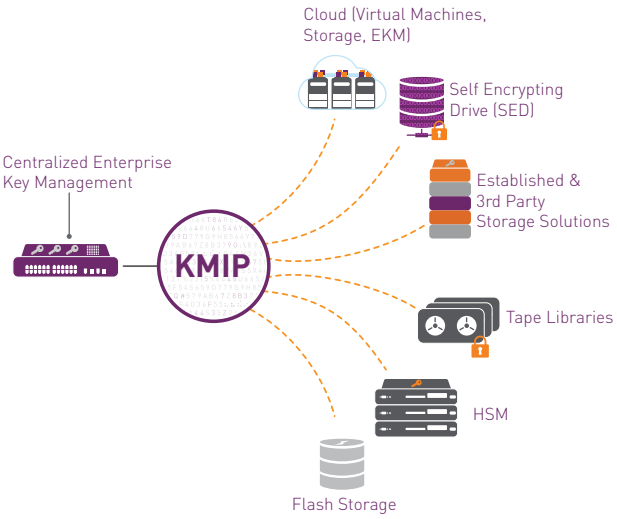
Providing Continuous Delivery of Automated and Cohesive Enterprise Key Lifecycle Management: Pre-Activation – Activation – Suspension – Revocation – Deactivation – Destruction – Compromise Recognition – and Compromise Destruction

As the number of these non-aligned enterprise storage encryption environments increase, essential monitoring and management of key state transitions throughout the keys' lifecycle are largely detached and opaque. By consolidating all key lifecycle management, enterprises can easily validate and verify any key state and key attribute changes for all encrypting storage solutions and their respective key management systems. The policies for these key state transitions can then be centrally monitored, controlled, and logged.

To deliver this continuous key lifecycle management, a centralized EKM system should provide support for components, protocols, standards, implementation choices, and policies included in the National Institute of Standards and Technology (NIST) Special Publications 800-57 - "Recommendations For Key Management", and 800-130 - "A Framework For Designing Cryptographic Key Management Systems".

Using the Organization for the Advancement of Structured Information Standards (OASIS) Key Management Interoperability Protocol (KMIP) for Standards-Based Systems Unification

Point encryption solutions have forced administrators to manage and maintain a swelling number of keys for multiple encryption types and multiple encryption devices. Consolidated management of these point solutions is imperative – and a standards-based protocol to facilitate this federation is now available: KMIP. KMIP defines the mechanisms for encryption client, device and key management server communications and corresponding key lifecycle operations. Using KMIP, an enterprise will be able to combine key management functions into a centralized EKM, allowing reduction of operational costs while enhancing its security controls and its overall security posture and policy governance. A centralized EKM system should ideally offer a Software Development Kit (SDK) and Application Programming Interface (API), allowing KMIP extensibility to both an organization's legacy storage encryption devices, as well as a wide assortment of other existing, and future, enterprise cryptographic environments.



Core Attributes of a Scalable Centralized EKM System

Within an effective centralized EKM system, key lifecycles must be structured and policy-driven, and key states must be centrally monitored and managed. The platform should be able to handle all cryptographic implementations for an enterprise, and be extensible to that enterprise's various systems, applications, and networked infrastructure.

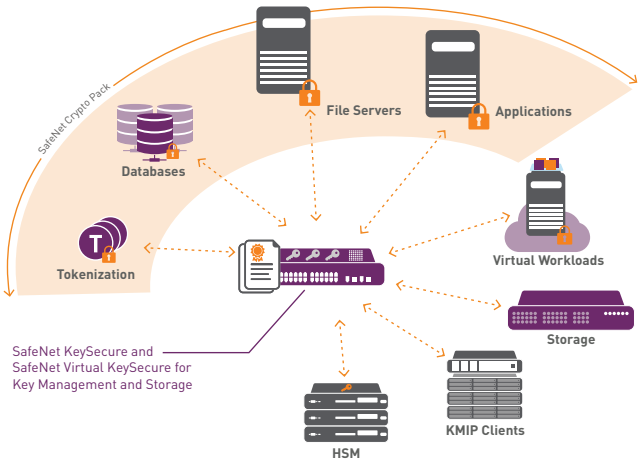
The following are principal centralized EKM platform attributes:

- **Consolidated Monitoring and Management of Key Lifecycle State Transitions.** As previously mentioned, centralized management of all key lifecycle states – pre-activation, activation, suspension, revocation, deactivation, destruction, compromise recognition, and compromise destruction – for all encryption keys must be visible and manageable from the enterprise key management platform's "single pane of glass". All related key transport between key management systems and encrypting storage systems must also be protected. This calls for strong identification, authentication and encrypted transport of all device-to-device communications and key material exchanges.
- **Direct System Administration and Role-Based User Access Control with Directory Services and Identity Management Infrastructure Integration.** The centralized EKM's administration roles and responsibilities must be partitioned and controlled to only permit those that have explicit authorization with privileged system access. A variety of multi-credentialed authentication techniques should also be supported. Furthermore, the EKM, through standardized communication exchange protocols, should be able to successfully integrate with an enterprise's directory services and identity management infrastructure. The system must be able to support an enterprise's granular, distributed, and role-based user access control. The enforcement of segregation of duties and principles of least privilege access, common to most mature organizations' security and compliance policies, are dependent on these attributes for any kind of successful implementation and regulatory compliance.
- **Consolidated Systems Logging and Reporting.** Secure, automated, and unified logging and reporting are absolutely crucial to maintain an organization's requisite risk and compliance posture. Key ownership must be clearly defined, and key lifecycle management and all modifications recorded and securely stored to provide an authentic and trusted audit trail of key state changes. EKM administrators and security personnel should also be alerted if attempts to breach protected keys occur.
- **Very High Availability and Scalability.** Enterprises need the centralized EKM platform to support high availability with fault-tolerant, auto-replicating, redundant failover capability. For this functionality, it should support active-active mode of synchronization, distributed / multiple geographies, and hierarchical clustering. The centralized EKM system must be able to scale to accommodate and manage the thousands, sometimes millions, of keys

throughout their lifecycles. An integrated Hardware Security Module (HSM) also helps assure that the EKM system's cryptographic keys are continually protected and available.

- **Exceptionally High Performance – with Very Low impact.** Cryptographic operations, especially those conducted at infrastructure concentration points like at a centralized enterprise key management system, are inherently computationally expensive. Therefore, co-processing of these functions is imperative. A hardened, self-contained, high-performance hardware appliance platform with integrated HSM is indispensable to ensure that little to no performance degradation is experienced at these focal points, and / or by the infrastructure at large.
- **Role-Based and Direct Access Control with Directory and Identity Management System Integration.** It must allow for strongly authenticated key management system logon, tiered administration, distributed policy, and separation of duties and principle of least privilege enforcement. To fulfill these requirements, the centralized EKM platform must support LDAP / AD directory services and identity management infrastructure. Secure client registration and communications for all exchanging of keying material must also be supported.
- **Gemalto SafeNet Crypto Operations Upgrade Pack (SafeNet Crypto Pack)** enables Gemalto SafeNet KeySecure to be used for encryption of structured or unstructured sensitive enterprise data residing in a server in the data center (physical, virtual, or cloud-based) or in the distributed enterprise. Data can be encrypted at the application, database column, file-system, virtual machine, or storage levels.

SafeNet Crypto Pack Solutions



Conclusion

A centralized EKM is fundamental to enterprise storage security. But the reality today is that the gaps between the legacy encryption islands continue to widen, making an enterprise's risk management and compliance programs ever more complex, laborious and costly. An enterprise continuing down this path will almost certainly find it increasingly taxing – and precarious.

The solution is clear: an automated, robust, centralized EKM system that can be easily deployed, is extensible to virtually any cryptographic security solution that uses interoperability protocol standards like KMIP, and can scale to cohesively manage the affiliated lifecycles of the exploding number of keys generated by these disparate encryption systems. For these adopting organizations, it will also pave the way for much smoother future storage security planning and deployment.

About Gemalto's SafeNet Identity and Data Protection Solutions

Through its acquisition of SafeNet, Gemalto offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy industry-leading protection of data, digital identities, payments and transactions – from the edge to the core.

Gemalto's newly expanded portfolio of SafeNet Identity and Data Protection solutions enables 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.

Through 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 www.safenet-inc.com
Follow Us: data-protection.safenet-inc.com

GEMALTO.COM

gemalto
security to be free