Vormetric Key Management

Simplifying IT Operations, Securing and Controlling Access to Data across the Enterprise
Executive Summary

Protecting the enterprise’s valuable digital assets from accidental or intentional misuse are key goals for every IT team today. Many organizations have deployed a variety of point encryption solutions as a primary method of protecting this data, and to meet various compliance mandates and internal data governance requirements. But unfortunately, the majority of these disparate encryption solutions have fallen short in their ability to address the enterprise’s key management challenges.

This white paper will take a quick look back at the evolution of encryption and integrated key management systems. IT operations and support challenges for encryption systems will then be examined, including regulation and compliance, complexity, lack of proper management tools, and ensuring availability and scalability. This is followed by a review of the recent industry initiatives and compliance regulations that are shaping the future of key management.

The paper will conclude with a brief introduction to Vormetric Key Management, describing how this powerful, integrated solution can enable IT to ensure the availability, security, and manageability of encryption keys across the enterprise.

Introduction

Pick up any information industry publication from the last five years and you’ll see multiple articles about the issues surrounding data security and management. These articles outline the costs associated with a breach of security, including hefty fines, loss of customer confidence and revenue, and the requirement for incremental (and often inefficient) resources to prevent these kinds of breaches in the future.

Recent industry research1 reveals that the average cost of a data breach is in excess of $7.2M per episode – a significant hit for any organization’s bottom line. Costs include payments for improved monitoring systems, notification to customers with breached data, and loss of revenue and brand loyalty.

There has also been a rapid increase in the number and complexity of compliance regulations that mandate improved controls and security management visibility, including the U.S. Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry Data Security Standard (PCI DSS). Heavy fines and other restrictive measures are levied on organizations with inadequate data protection that can range from $250K to upwards of $20M per event. These problems have now moved encryption into the forefront as a method of securing data throughout its lifecycle.

Overview of Key Management Systems

The Internet has been the most significant driving force in the evolution of key management systems. The connection of public and private sources has provided much easier access to the organization’s network and data to those who need it – notably employees, customers, prospects, and partners. But it has also opened the door to intentional or accidental misuse by hackers or even malicious internal users. These attacks can have dire consequences for the enterprises under siege, resulting in substantial loss of revenue, massive fines, and degraded customer trust.

A variety of security policies, including a multitude of methods, controls, compliance laws, and regulations, were developed to battle these forces. Data encryption moved from its initial focus as a tool primarily for the military, into the industry as whole, serving as an effective way to fight these intruders. As attacks became increasingly more sophisticated, the data processing industry began improving these early encryption systems, eliminating the difficulties of disparate native key repositories that were then scattered across the various information systems in the enterprise. These difficulties included the inefficient use of resources, lack of management control and visibility, poor key security, and the requirement for ever-increasing regulatory control and reporting.

“While the implementation of encryption is complex, conceptually it is easy to understand. The final encrypted solution has two parts: the encrypted data itself and the keys that control the encryption and decryption processes. Controlling and maintaining the keys, therefore, is the most important part of an enterprise encryption strategy. Encryption methods and algorithms are standardized and well understood, but key management is unique to each organization.”


Data Encryption: Integrated vs. Third-Party Key Management Systems

The increased adoption of encryption solutions has improved security for enterprises, but it has made life much more challenging for the IT security team, now tasked with the management and control of a variety of encryption keys.

Nearly all offline data storage devices include an option of an embedded encryption capability. At the same time, many database management systems (DBMS) and application software providers also offer native encryption options. A challenge with these disparate islands of encryption is that keys and key management software from each provider don’t usually interoperate well with those of other IT providers.
The resulting silos of security, where system administrators and database administrators (DBAs) have to become the managers of the encryption keys for a particular system, distracts from their primary tasks of IT or database administration. Along with the resource inefficiency of such a methodology, it also puts an enterprise’s overall security posture at risk.

While there are a variety of encryption systems requiring key management, two major approaches have emerged:

**Integrated Key Management Systems**
Integrated key management systems are built in to a specific encryption solution, including functions such as generation, storage, backup, authentication, security, audit, key state management, and restoration. Encryption solutions (such as Vormetric Encryption) provide a combination of encryption and key management in one integrated package.

**Third-Party Key Management Systems**
Third-party key management systems are used for encryption systems providing no or limited integrated key management. A third-party key management system provides one or all of the functions provided by an integrated key management system (generation, storage, backup, authentication, security, audit, key state management, and restoration) with the exception of authentication. The encryption system must authenticate and request a key from the key management system based on its particular system specific needs. Examples of where third-party key management systems are typically found include the Transparent Data Encryption (TDE) found in databases such as Oracle 11gR2 and Microsoft SQL Server.

Enterprises frequently have some combination of the two approaches deployed in their environments, but are finding that consolidating and centralizing key management improves visibility and increases control across the enterprise, reduces key management costs, and minimizes compliance headaches.

**Interoperability Standards and Initiatives: PKCS#11, EKM, and OASIS KMIP**

Complex technologies with a variety of approaches often need interoperable standards and openness to enable users to obtain the best and longest-lasting benefits from their use. This is definitely true with the use of cryptographic systems. Even though vendors may agree on many of the basic cryptographic techniques and standards, compatibility between key management implementations is by no means guaranteed.

Three important industry standards to ensure interoperability are:

**PKCS#11**—Public Key Cryptographic Standard #11 specifies an API, called Cryptoki (short for cryptographic token interface), to devices that hold cryptographic information and perform cryptographic functions. RSA Laboratories developed this standard in cooperation with representatives of industry, academia, and government. Cryptoki follows a simple object-based approach, addressing the goals of technology independence for any device as well as resource sharing for multiple applications accessing multiple devices. It presents to applications a common, logical view of the device called a cryptographic token. PKCS#11 is used by Oracle Transparent Data Encryption.
EKM/MSCAPI – The Microsoft SQL Server database provides data encryption capabilities and enables secure key management with third-party key management providers through Extensible Key Management (EKM) using the Microsoft Cryptographic APIs (MSCAPI). Keys for data and key encryption are created in transient key containers. They must be exported from a provider before they are stored in the database. This approach enables key management that includes an encryption key hierarchy and key backup for Microsoft SQL Server Transparent Data Encryption.

OASIS KMIP – OASIS, the independent Organization for Advancing Open Standards for the Information Society, is the standards body sponsoring the initiative to adopt the Key Management Interoperability Protocol (KMIP). Architects, designers, implementers, providers, and consumers of enterprise key management systems have come together to define a single, comprehensive protocol for communication between encryption systems and a broad range of new and legacy enterprise applications, including email, databases, and storage devices. By removing redundant, incompatible key management processes, KMIP will provide better interoperability. The specification addresses anticipated customer requirements for key lifecycle management, key sharing, and long-term availability of cryptographic objects of all types, including public/private keys and certificates, symmetric keys, and other related areas.

The Challenges of Encryption Key Management

Most IT organizations have gradually adopted disparate systems with different ways of managing encryption keys over many years. It may be a security breach event, the burden of managing disparate encryption systems, the trauma of a lost encryption key that renders data inaccessible, or an industry compliance regulation that forces them to turn to key management as a requirement for improving data security.

In the May 11, 2011 issue of TEST2 (an industry publication that follows issues affecting the software testing market), survey results revealed that 40 percent of IT staff admitted that they could hold their employer hostage – even after they left for other employment – by making it difficult or impossible to access vital data by withholding or hiding encryption keys. A third of survey respondents said that their knowledge of and access to encryption keys and certificates, used for both system authentication and data protection, meant they could vitally affect their company’s financial and reputational well-being with minimal effort and little to stop them. This was attributed to lack of oversight and poor management of their organization’s encryption keys.

Nearly a third of the respondents said that they could still access organizational data because they could easily retain the encryption keys when they left and had found ways to access the information remotely. Many said they would use an automated solution to encryption key management –”if they knew it existed.” This survey crystallizes the pressing need for IT organizations to mitigate risk by using effective and efficient key management systems for the protection of their companies’ mission-critical data.

The following sections will review several of the challenges IT organizations face when trying to control and manage their plethora of encryption keys.

2 https://www.pcisecuritystandards.org/pdfs/pci_ptp_encryption.pdf
Complex and Messy Management

Without a centralized system of encryption key management, security administrators are faced with a costly, inefficient, and often impossible task. A typical enterprise has accumulated many different databases over time from separate vendors. This heterogeneous world means that an enterprise looking to secure databases, such as Oracle and SQL Server with native Transparent Data Encryption (TDE), has to factor in the increased costs and administrative resources required for managing multiple, incompatible encryption solutions. In addition, each separate encryption system requires specialized training to learn the unique processes that are specific to that system.

Many database vendors provide minimal key management functionality and point to network Hardware Security Modules (HSMs) to provide the necessary key management. Such key management functionality can become costly when enterprises need to wrestle with large deployments involving tens or even hundreds of servers, each having a separate encryption key to manage, but the key management infrastructure does not scale to a similar degree.

Without an enterprise-wide key management system to apply consistent security, each system administrator separately controls the keys, leaving room for security compromises such as putting encryption keys next to encrypted data – the electronic equivalent of taping the key to the front door. Manual systems to store and transmit the keys, lack of password control, and the failure to secure keys when an employee leaves the company are typical data breaches waiting to happen. And strict adherence to compliance requirements is nearly impossible in this situation.

“External key managers handle key sharing, backup, and other services that would otherwise be handled automatically by the database itself. Most customers we speak with now opt for dedicated hardware to support key management operations.”


Ensuring Encryption Key Security

Ensuring the security of encryption keys is perhaps the single most important part of an IT system’s security umbrella. Keys are vulnerable to attacks from outside hackers and malicious insiders, and at every point in the key lifecycle of generating, storing, rotating, using, verifying, distributing, and ultimately retiring or destructing compromised old keys.
As with any important organizational function, key management begins with a unified strategy and a description and dissemination of proper policies and procedures. Every step in the lifecycle above must be carefully managed and controlled. An effective enterprise key management system can provide the tools, as well as the visibility and reports to undertake this task. Such a system must be able to scale as the company grows, but also be flexible enough to allow for the adoption of new technologies and industry standards as they emerge. Key security is not only important for thwarting costly cyberattacks; it is also a mandatory part of compliance regulations.

**Guaranteeing Availability**

Organizations cannot function without the availability of their essential data and information. It stands to reason that the most important data for the functioning of the business is the most likely to need encryption for security. That important encrypted data must be easily accessible to authorized users, so a well-designed key management system must provide high availability. For a user, be it an employee, customer, or business partner, loss of availability of data due to a key management failure is no different from complete loss of data due to a hardware failure.

A key management system reduces the complexity of key administration, which ultimately reduces mistakes and security lapses, which in turn helps maintain the availability of data. But there are other components of key security systems that address high availability. Redundant, high availability key appliances are utilized, with all key activities and access controls mirrored in real time to a separate, fail-over key appliance.

**Enabling Scalability and Flexibility**

The growth in complexity and size of an organization's IT system can result in a similar increase in the requirement for data security. A key management solution must be able to scale with the organization’s business needs. Scalability in this context means the ability to support large numbers of database instances (e.g., in the thousands). IT infrastructure and security are also changing at a rapid pace due to a steady flow of new applications and evolving compliance mandates. A key management solution must provide the flexibility to adapt to changing requirements.

**Facilitating Governance and Reporting**

Shareholders, customer contracts, and government entities can all mandate an organizational information governance system. The consequences of poor governance can be huge, with large fines, shareholder suits, and loss of customer loyalty. The most important aspect of governance is a discipline for managing, controlling, and protecting the security and privacy of data. Encryption key management systems are a major part of this discipline.

A policy-driven key management system forces the adherence to procedures for separation of duties and user authorization, and it automates all the security processes involved in the key lifecycle. Management reports il-
luminate problem hotspots and vulnerabilities, unlike native key management solutions within databases, which merely store and retrieve keys for authorized users. Database vendors providing native database TDE who point to HSMs to provide the necessary key management cannot meet these regulatory requirements.

Some of the more notable industry standards and requirements affecting key management today include:

**The Payment Card Industry Data Security Standard³ (PCI DSS)** requires encryption key management systems with controls and procedures for managing key use and performing decryption functions.

**The Gramm Leach Bliley Act (GLBA)** in the United States requires that firms acknowledge publicly when an disclosure event occurs, taking whatever damages to their reputation or market position that such a statement would entail. Led by California’s Database Security Breach Notification Act in 2003, more than half of all states have passed additional rules beyond the general notification requirements of GLBA to require firms to notify disclosure victims of the event, with higher associated costs to the business than GLBA exacted.

**The U.S. Health Information Technology for Economic and Clinical Health (HITECH) Act** includes a breach notification clause for which encryption provides safe harbor in the event of a data breach. For “unsecured protected health information” that is not secured by a technology the renders the information unusable, unreadable, or undecipherable (i.e., encryption technology), notification of the breach to every individual affected must be made.

Breach liability, now widely embraced, adds even more incentive to governance risk and compliance (GRC) managers within corporate organizations to require the development of data protection and encryption strategies going forward. With the continued increase in regulations, the need for strong key management systems is becoming more and more important.

### Introducing Vormetric Key Management

Vormetric Key Management (VKM) provides a robust, standards-based platform for managing encryption keys from disparate sources across the enterprise. It simplifies the management and administrative challenges around encryption key management to ensure that keys are secure and always provisioned to authorized encryption services.

Vormetric Key Management enables enterprises to:

**Improve Operational Efficiency.** VKM ensures that keys are stored securely and always available to authorized encryption services. It also provides the ability to audit and report on all activities relating to keys including key generation, rotation, destruction, key import, and key export.

**Reduce Management Burdens with Centralized Key Management.** VKM simplifies the process of managing cryptographic keys, enabling security teams to gradually consolidate the management of encryption across the enterprise. Centralized key management in a solution confirming to FIPS 140-2 that allows adminis-
Cut Costs with a Unified Solution. VKM enables enterprises to minimize encryption key management costs by managing heterogeneous encryption keys, including keys generated by Vormetric Encryption, IBM InfoSphere Guardium Data Encryption, Oracle TDE, Microsoft SQL Server TDE, and other applications with integrated encryption. VKM shares common infrastructure with Vormetric Encryption, enabling customers to use a common Data Security Manager appliance to control Vormetric Encryption along with other encryption solutions.

Vormetric Key Management Elements

Vormetric Key Management is part of the Vormetric Data Security family of offerings. VKM manages third-party encryption keys, while Vormetric Encryption combines server encryption for data-at-rest with integrated key management. Both Vormetric Key Management and Vormetric Encryption share common management and system infrastructure.

Figure 1. Vormetric Key Management Elements.

The following three elements comprise the Vormetric Key Management solution:

Vormetric Data Security Manager (DSM) is a network Hardware Security Module (HSM) appliance that provides centralized key and policy management. It features an intuitive Web-based management console for enterprise-wide administration, policy management and audit of encryption keys. The Vormetric DSM conforms to FIPS
140-2 and provides common management for both Vormetric Key Management and Vormetric Encryption.

Vormetric Key Agents integrate with Oracle TDE and Microsoft SQL Server TDE and communicate with the Vormetric Data Security Manager to provide lifecycle management for Oracle TDE Master Encryption Keys and Microsoft SQL Server database encryption keys.

Vormetric Key Vault provides high availability storage and backup of symmetric and asymmetric encryption keys of any strength, and tracks expiration dates. Key Vault is an option available with the Vormetric Data Security Manager.

**Summary**

Data is only as secure as the system that manages the encryption keys protecting the data. A centralized enterprise key management solution is critical to ensuring all sensitive enterprise data is secure and available.

Vormetric Key Management is the only solution today that can minimize IT operational and support burdens for encryption key management, secure and control access to data across the enterprise and into the cloud, and protect data – without disrupting or changing any existing application or database environments.

**About Vormetric**

Vormetric is the leader in enterprise system encryption and key management. The Vormetric Data Security product line provides a single, manageable, and scalable solution to manage any key and encrypt any file, any database, any application, anywhere it resides—without sacrificing application performance and avoiding key management complexity. Some of the largest and most security conscious organizations and government agencies in the world, including 15 of the Fortune 25, have standardized on Vormetric to provide strong, easily manageable data security. Vormetric technology has previously been selected by IBM as the database encryption solution for DB2 and Informix on Linux™, Unix® and Windows; and by Symantec to provide the Symantec Veritas NetBackup™ Media Server Encryption Option.

For more information on Vormetric Key Management, please call (888) 267-3732 or visit [www.vormetric.com](http://www.vormetric.com).