thalescpl.com

THALES

Thales Key Management

Securing data across the enterprise while simplifying IT operations

White Paper

Contents

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 their data and to meet various compliance mandates and internal data governance requirements. Unfortunately, however, the majority of these disparate encryption solutions have fallen short in their ability to address the enterprise's key management challenges.

This white paper starts with a look back at the evolution of encryption and key management systems. The challenges for IT teams around encryption systems are then 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 concludes with an introduction to Vormetric Key Management from Thales, describing how this powerful, integrated solution can enable IT to ensure the availability, security, and manageability of encryption keys across the enterprise.

Data Security Challenges

Many organizations are adopting digital transformation to drive efficiency into their data-intensive processes. With this shift to a data driven world, 94%[1] of organizations are using sensitive data in cloud, big data, IoT, containers or mobile environments, which in turn creates new attack surfaces and drives the need for evolving data security approaches. At the same time, breaches continue to threaten the landscape at an increasing rate.

> **"Successful breaches have reached an all-time high for both mid-sized and enterprise class organizations, with more than two-thirds (67%) of global organizations and nearly three fourths (71%) in the U.S. having been breached at some point in the past. Further, nearly half (46%) of U.S. respondents reported a breach just in the previous 12 months, nearly double the 24% response from last year, while over one-third (36%) of global respondents suffered a similar fate."**
>
> -Garrett Bekker, 451 Research Principal Analyst, Information Security Author of the 2018 Thales Data Threat Report

Meeting data security challenges, particularly in the age of digital transformation, while maintaining operational efficiency, is a major goal for today's enterprises.

Encryption and Key Management Techniques—a brief look back

The Internet has been the most significant driving force in the evolution of encryption and key management systems. The connection of public and private resources 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.

In response to the emergence of the Internet and its data threats, 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 a whole, serving as an effective way to fight these intruders. As attacks became 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.

1. **Thales Global Data Threat Report, 451 Research, 2018;** http://go.thalesesecurity.com/rs/480-LWA-970/images/2018-Data-Threat-Report-Global-Edition-ar.pdf

Data Encryption across Disparate Systems—Silos of Security

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 managing a variety of cryptographic keys.

Nearly all offline data storage devices include the 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 islands of encryption is that keys and key management software from each provider don't usually interoperate well with one another.

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 and database administration. Along with the resource inefficiency of such a methodology, it also puts an enterprise's overall security posture at risk.

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 using native 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.

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 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. "**
>
> - Securosis: "Understanding and Selecting a Database Encryption of Tokenization Solution"[2]

2. **Securosis: "Understanding and Selecting a Database Encryption of Tokenization Solution"; https://securosis.com/assets/library/reports/Securosis_Understanding_DBEncryption.V_.1_.pdf**

Meeting Today's Challenges: Key Management Essentials

Key management requires a number of elements in order to be successful in the face of the challenges described above. These elements are described below.

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 at every point in the key lifecycle of generating, storing, rotating, using, verifying, distributing and ultimately retiring or destroying 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 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, and also be flexible enough to allow for the adoption of new technologies and industry standards as they emerge. Additionally, 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 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 also 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.

Centralizing Key Management

To address the challenges of key management for disparate encryption systems which can lead to siloed security, two major approaches to centralizing key management have emerged:

Integrated Key Management Systems

Integrated key management systems are built into a specific encryption solution, including functions such as generation, storage, backup, authentication, security, audit, key state management, and restoration. Encryption solutions (such as Vormetric Transparent 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 that provide no or limited integrated key management. A third-party key management system provides one or all of the functions delivered by an integrated key management system including generation, storage, backup, security, audit, key state management and restoration, and further offers the benefit of managing keys for multiple encryption systems simultaneously while centralizing the process. For example, third-party key management systems can complement Transparent Data Encryption (TDE) used with Oracle and Microsoft SQL Server, among others.

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.

Adhering to Industry Standards

Complex technologies often rely on interoperability standards to help users obtain the easiest and longest-lasting benefits from their use. This is certainly true for cryptographic systems, where important industry standards designed to ensure interoperability have been established. A successful key management system will interface with these standards to ensure wide usability. The following are three chief interoperability standards that are used today:

PKCS#11–Public Key Cryptographic Standard #11 specifies an API for devices that hold cryptographic information and perform cryptographic functions. RSA Laboratories developed this standard in cooperation with representatives of industry, academia, and government. PKCS#11 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. As an example, PKCS#11 is used by Oracle TDE.

EKM/MSCAPI – The Microsoft SQL Server database provides data encryption capabilities and enables secure key management by third-party providers through Extensible Key Management (EKM) using the Microsoft Cryptographic APIs (MSCAPI). Keys for data and key encryption are created in transient key containers. The keys 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 that founded and maintains the Key Management Interoperability Protocol (KMIP). Architects, designers, implementers, providers and consumers of enterprise key management systems collaborate to maintain 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 improves interoperability. The protocol addresses 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.

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.

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

General Data Protection Regulations (GDPR)

Perhaps the most comprehensive data privacy standard to date, GDPR affects any organization that processes the personal data of EU citizens - regardless of where the organization is headquartered. The GDPR is designed to improve personal data protections and increase organizational accountability for data breaches. With potential fines of up to four percent of global revenues or 20 million EUR (whichever is higher), the regulation has impact on many businesses.

UIDAI's Aadhaar Number Regulation Compliance

The Unique Identification Authority of India (UIDAI) was established under the provisions of India's 2016 Aadhaar Act. UIDAI is responsible for issuing unique identification numbers (UIDs), called Aadhaar, and providing Aadhaar cards to all residents of India. The 12-digit UIDs are generated after the UIDAI verifies the uniqueness of enrollees' demographic and biometric information; UIDAI must protect individuals' identity information and authentication records.

The Payment Card Industry Data Security Standard (PCI DSS)

Any organization that plays a role in processing credit and debit card payments must comply with the strict PCI DSS compliance requirements for the processing, storage and transmission of account data. The PCI DSS standard involves assessment against over 200 tests that fall into 12 general security areas representing six core principles. These PCI DSS tests span a wide variety of common security practices along with technologies such as encryption, key management, and other data protection techniques.

The Gramm Leach Bliley Act (GLBA)

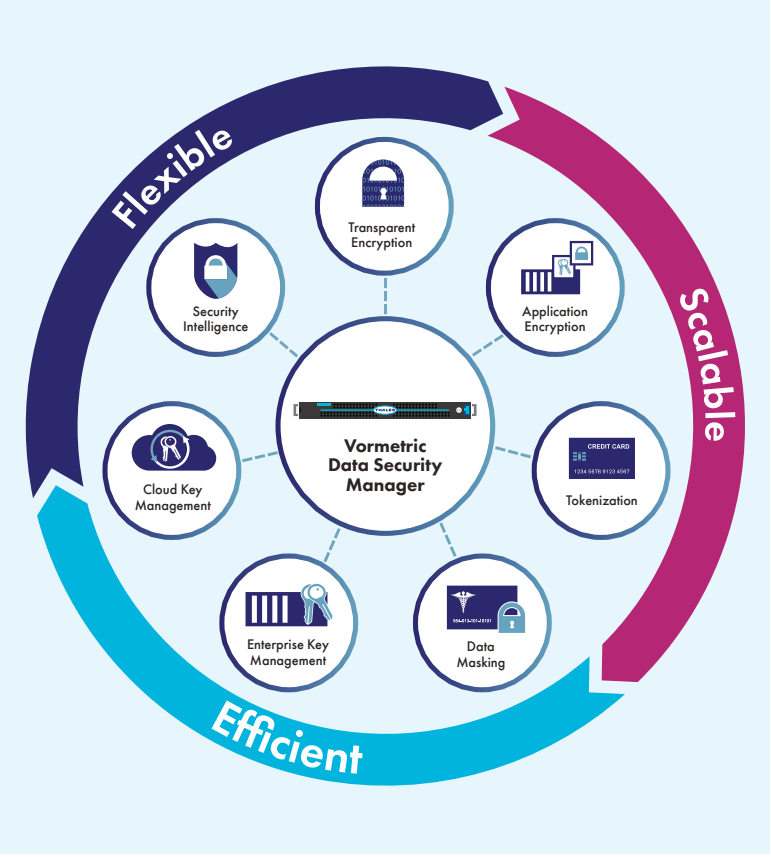
In the United States requires that firms acknowledge publicly when a disclosure event occurs, taking whatever damages to their reputation or market position that such a statement would entail. Led by California's Database Security Breach Notification Act in 2003, more than half of all states have passed 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 that 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 becomes more and more important as every encryption strategy requires a correspondingly strong key management system to underpin its security.

Thales Key Management Solutions



The Vormetric Data Security Platform features multiple data security products that can be deployed individually or in combination to deliver advanced encryption, tokenization and centralized key management.

Vormetric Key Management (VKM) from Thales provides a robust, standards-based platform for managing encryption keys from disparate sources across the enterprise. It simplifies the 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.

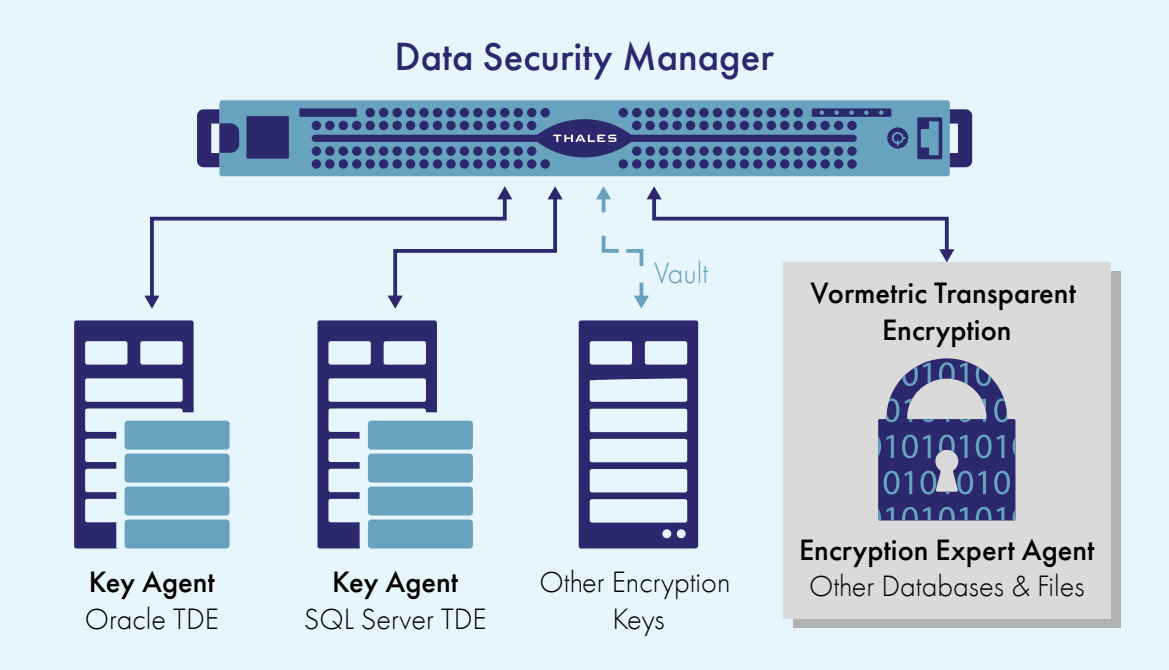
Cut Costs with a Unified Solution. VKM enables enterprises to minimize security administration costs by managing, using a single solution, encryption keys used by a variety of applications such as Vormetric Transparent Encryption, IBM Guardium Data Protection, Oracle TDE, Microsoft SQL Server TDE, KMIP clients and other applications.

Vormetric Key Management Elements

Vormetric Key Management is part of the Vormetric Data Security Platform family of offerings. VKM manages third-party encryption keys, while Vormetric Transparent Encryption provides encryption services combined with integrated key management. The Vormetric Data Security Platform, as shown in Figure 1, encompasses a variety of encryption tools which lets customers easily expand their security portfolio using a single platform.

The following three elements comprise the Vormetric Key Management solution:

- At the core of the Vormetric Data Security Platform, the Vormetric Data Security Manager (DSM) is an appliance that provides centralized key and policy management to a variety of applications, as illustrated in Figure 2. The DSM features an intuitive Web-based management console for enterprise-wide administration, policy management and audit of encryption keys. The Vormetric DSM is certified to FIPS 140-2 and provides common management for Vormetric Key Management, Vormetric Transparent Encryption and a wide variety of other agents and functions.
- 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.



Vormetric Key Management Elements.

Thales Hardware Security Module Partner Solutions

Thales partners with a wide variety of strategic partners who use hardware security modules (HSMs) as the high assurance root of trust for their IT solutions. HSMs are hardened, tamper-resistant security devices that generate and protect strong cryptographic keys used for a variety of purposes. A sample use case is integrated, turnkey key lifecycle management services where the HSM generates keys and safeguards them in its FIPS 140-2 hardware environment.

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 from Thales and HSMs help organizations maximize IT efficiency through a centralized, extensible platform-based solution, and support the burdens of encryption key management across the enterprise and into the cloud – without disrupting existing application or database environments.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing amount of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

THALES

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: asia.sales@thales-esecurity.com

Europe, Middle East, Africa
Meadow View House, Long Crendon,
Aylesbury, Buckinghamshire HP18 9EQ
Tel: +44 (0)1844 201800 | Fax: +44 (0)1844 208550
E-mail: emea.sales@thales-esecurity.com

> thalescpl.com <