Industry Must-Haves for Effective Encryption Key Management

DATA SECURITY HAS COME A LONG WAY within just the past few years. Organizations no longer have to continue to maintain current patchwork methods because there are no available, cost-effective, or interoperable solutions that easily solve their problems. Encryption and encryption key management are now industry standards and work across both legacy and newer business systems, multi-platform and multi-tenant networks, remote access workstations, geographical offices, data centers, and third-party business partners.
Executive Introduction

Business environments have evolved to become extensive ecosystems pulsing with sensitive data. This data requires continuous and effective protection while it is stored or transferred during any dynamic transaction all the way through to storage, archival, and successive access. Third-party business relationships and in-house business intelligence who endeavor to manage the data increase the number of business and system transactions as well as personnel access to private and confidential information. When data is breached, organizational leaders come under immediate scrutiny for their commitment to secure this information. Information is the lifeblood of business, and strong protection of data is a constant task since data gets out. It’s a daily dilemma for chief security officers, regulatory and compliance auditors.

Security professionals and business leaders alike are experiencing the ramifications of data breaches due to aging implementations, lack of consistently implemented controls and processes, and risk management evaluations. Customers and business partners often end their relationship with these organizations due to these practices, and the company reputation is negatively impacted for years to come. Consumers within the industry also become wary of continuing to provide their private and confidential information to these organizations. Other businesses within the same vertical also come under scrutiny as to whether they have effective protection implementations in place. In other words, one organization’s breach has broader negative implications that can impact their entire industry. Business leaders are now working in concert with security professionals to better strategize, evaluate, fund, and prioritize data protection methodologies that prove effective and reliable within their complex environments. However, oftentimes these efforts are a reaction to a breach that has already occurred, as well as the consequences of that breach, including: intensive and costly forensic examination, litigation, customer communications and explanations, and paying fines associated with the breach.

Data security has come a long way within just the past few years. Organizations no longer have to continue to maintain current patchwork methods because there are no available, cost-effective, or interoperable solutions that easily solve their problems. Encryption and encryption key management are now industry standards and work across both legacy and newer business systems, multi-platform and multi-tenant networks, remote access workstations, geographical offices, data centers, and third-party business partners.

First, we’ll address the top three security needs business must address. We’ll outline how businesses can meet these needs using ‘must-haves’ such as industry standard encryption and key management, key management best practices, and solutions that are easy to use and cost-effective.

Top Three Needs to Solve

- I need a solution that’s affordable and quick-to-deploy.
- I need a key manager that distributes encryption keys across all my system platforms.
- I need an implementation with known costs and no additional professional service or connectivity fees.

Industry Must-Haves - Introduction

Secure socket layer (SSL) use internally and across the internet is common for datastream communications, but data at rest across various critical systems and data stores has proven problematic to protect due to interoperability issues for key management. To secure data at rest, two basic questions must be asked:

- What is the data workflow, and is the data protected throughout the handling process?
- Where is the data ultimately stored and how is it protected there?

Encryption for data at rest across the entire business environment typically involves disparate applications. With many applications often running on different platforms and operating systems, protecting data becomes a challenging and lengthy custom engineering process that has prevented organizations from encrypting all of their important data.

Before a business can locate their sensitive data and protect it, major roadblocks around acquiring an encryption and key management solution must be addressed. Database administrators must ask:

- How straightforward is the solution to install and implement?
What is the true cost of the product for protections it provides?
How reliable is the product within my complex data ecosystem?

The following encryption key management “must-haves” are critical components of a qualified, beneficial, and resilient solution that can answer these questions and pass necessary due diligence to protect data from a devastating data breach. Every business should evaluate these items and form questions to ask your current vendor as part of evaluating any improved key management.

The Principles of Effective Encryption Key Management

Management of Encryption Keys
Key management is not provided as part of encryption methodologies. Yet, the creation, management and protection of these encryption keys are the most critical aspects of maintaining confidentiality and privacy of transacted data at rest. Even if data is accessed without authorization, the data is illegible in encrypted format, thus secure key management is essential within an enterprise or cloud computing environment and includes these components:

- FIPS 140-2 compliant key management to best protect, store, and retrieve the encryption keys.
- Symmetric keys are securely transmitted through a tunnel established through secure TLS negotiation.
- Large numbers of keys are easily managed and deleted through a TLS secure session for strong, mutual authentication.
- Symmetric keys provide fast NIST validated AES encryption of data at rest within files and databases.
- Keys are not stored on the same system as the encrypted data and access to the keys restricted.
- Associated key events are logged and alerted upon using industry SIEMs.
- Encryption keys can be used throughout the application stack to encrypt data within the user interface, within the client, within middle tiers as well as databases, tapes, and SANs.
- A key manager allows management of a sufficient number of keys so that any one key only encrypts an appropriate amount of data.

Encryption Methodology
In addition to FIPS certification for key management, the software encryption algorithm utilized to convert plain text into unintelligible ciphertext must be strong, certified to stringent standards, and extensively community tested. Symmetric encryption is fast, and the Advanced Encryption Standard (AES) is validated by the National Institute of Standards Technology (NIST), extensively community tested, and is industry standard today.

FIPS 140-2 Validation
A hardware security module (HSM) is industry preferred only if it has been FIPS 140-2 validated. All resulting version upgrades must maintain FIPS 140-2 compliance, and substantial new changes require re-certification. Compliance with NIST FIPS 140-2 demonstrates the vendor not only stands behind their appliance and implementation, but they have ensured rigorous testing and evaluation by an approved top security organization to the highest levels of key management security standards. While it is not possible to perform FIPS 140-2 validation in a cloud service provider context, it is important that the key management software has been through validation on another platform.

Separate Encryption Keys from Users and Data
Encryption keys should never reside on the same server as the encrypted data. This practice is similar
to leaving the keys to your house under your welcome mat. A hardware security module for maintaining separation of encryption keys from the data that’s being encrypted is essential.

**Separation of Duties**  
A division of duties is essential so that the person creating and managing the key has no access to the protected data. Quite simply, the administrators who manage encryption keys and those who consume them (DBAs, users, business partners, etc.) must be separated. The administrator or cryptographic security officer creates and deletes the key but can’t encrypt or decrypt with it, and the database administrator on the other hand can encrypt or decrypt but can’t create or delete keys.

**Dual Control**  
Establishing dual control ensures two or more people are involved in the critical security tasks to reduce fraud or abuse. Additionally, changes must require authorization regarding adding and deleting keys.

**Generation of Encryption Keys**  
For decades there has been discussion of the best way to generate encryption keys. Administrators sharing a split encryption key or having a break-the-glass process have become less accepted practices due to the manual process often breaking down, and customers transacting their most confidential data prefer an automated process where no one individual can obtain portions or collude to access the full encryption key.

**Type/Size of Encryption Keys**  
The greater the size of the key type and the type of the key generated (i.e. AES) to encrypt clear text determines the work and time effort necessary to successfully complete a brute force attack. As computational processing improves, the greater the size of encryption keys are needed to sustain protections, and organizations require a solution that helps them readily move to a greater key size. Industry practice is to deploy AES symmetric keys with a minimum of 128 bit keys for fast and secure encryption processing.

**Key Lifecycle**  
The key lifecycle includes key establishment, activation, use, expiration, retirement, escrow and eventual retirement and destruction. Industry standard practice dictates encryption keys should be rotated so they are only active for a limited period of time, and then rendered disabled or deleted while new encryption keys are created and utilized. An organization’s key lifecycle strategy and configuration is elemental to strong key management. Also, industry thresholds such as those set by the Payment Card Industry Data Security Standard (PCI DSS) requires periodic key rotation, and best practice is to set it for a limited period of time for the strongest sensitive data protection.

**KMIP (Key Management Interoperability Protocol)**  
KMIP is an important part of an encryption strategy, as it provides an open industry standard for key management. Meeting the OASIS KMIP specification enables interoperable communication between cryptographic environments and key managers, reducing the operational, training, and infrastructure costs for key management in the enterprise.

**Extensibility**  
A key manager’s application program interface (API) is essential for extending and automating key management and encryption processes. A robust API enables scripting of processes across a wide range of activities, ensuring the key management solution is extensible for integrating deeper into a defense-in-depth environment.

**Checksums**  
A common computing technique used to determine the integrity of documents is applying a hashing function checksum that will indicate whether the data has been altered. The key used to generate tamper-indicating hashing checksums must be unique from the key to encrypt the data. An encryption key management solution that uses the same key for generating checksums as it does for data encryption is flawed. If it’s possible to retrieve the hashing key to verify computational values, and it’s the same key used to encrypt the data, then it’s possible to obtain the key to decrypt the data through the engineering rasterization process. If this realization doesn’t concern your organization, it’s sure to concern your customers and business partners whose data the organization has the privilege of transacting and managing.

**Virtual and Cloud Compliance**  
Virtual servers enable enterprises to lower operational costs and spin up additional computing power to meet user needs, deploying encryption key management
in the cloud, and accelerating deployment of mission critical security technology. The key manager should align with evolving NIST guidance on FIPS 140-2 compliant encryption key management software for virtual instances, and expanding Cloud Security Alliance requirements for STAR certification. In multi-tenant, shared environments, encryption key management provides a form of isolation and privacy of information from other commingled, customer data, especially when the organizations controls and manages the keys within a hybrid cloud.

**Extensive Virtual Environments**
In today’s extensive computing environments, key management needs to stay current with virtualization efforts for greater on-demand computing responsiveness. For the greatest flexibility within evolving virtual environments, select a key manager capable of running on a virtual machine, managing keys to a dynamic cloud, and virtual machine instances in the cloud for greater deployment and management flexibility.

**Authentication Options**
While username and strong passwords are still the most common form of authentication in use, many organizations have invested in multi-factor authentication schema, which can include PKI, smart cards, tokens (hardware and software), biometrics (face, fingertip, palm, retina), phone authentication, knowledge-based authentication, and certificate authentication of server admins. A leading encryption key management solution allows for the integration of your preferred method of authentication.

**Mutual Authentication for Administration**
Encryption key exchange for establishing secure administration and data transmissions have long evolved past SSL to TLS. The importance of TLS can’t be underscored – in addition to any authentication mechanism the organization or third-party may provide and establishing a secure session for data exchange, TLS provides strong mutual authentication between systems to prevent a man-in-the-middle attack of someone trying to sniff, redirect or impersonate the intended recipient or rogue system.

**End of SSL/TLS Tunnel**
Not all SSL/TLS sessions end in a secure zone. What happens with the workflow of the data across all possible transactions and through to the database or archival storage are vital components in any end-to-end encryption design.

**System Logging/Monitoring and Audit Trail for Compliance**
The ability to log the administration and retrieval of keys, and generating a secure audit trail of management activities and use of keys is a primary requisite. Security Information and Event Management (SIEM) is accomplished through system logging. The first test auditors perform is evaluating if the generated audit and logging trail exists, and whether or not logs can be altered.

**Centralized and Distributed Environments**
The encryption key management solution must be robust and timely failover should be inherent in the key manager design, to fully function within a primary production site and the associated warm sites across multiple, geo-diverse remote and cross-continental sites (i.e., data centers, offices and call centers across regional, national, and global environments.) Additionally, key management HSMs must implement hardware redundancy such as hot-swappable RAID disk drives, redundant power supplies, etc.

**Usability**
The current industry buzzword of “disruptive” technology doesn’t apply to encryption key management. Use must be consistent, reliable, and resilient, utilizing current best practice methodologies to be dependable now and with the changing systems and infrastructures in the future. The goal of encryption key management is to base it on tried, tested, and trusted standards to enable the securing of information in an everyday easy, reliable, and automated practice – without exceptions having to be made for the user, application system, or network environment.

**Professional Services for Customization**
Custom integration is a factor for key management. As part of any installation, verify if there is a professional service integration cost or additional connectivity costs on top of the purchase price. Ensure that the integrations will work across all of your critical systems require encryption key management. A solid and trusted vendor, no matter their size, will put the extra effort forward at no cost to ensure their product functions reliably and as promised.

**Human-Centered UI Design**
While systems should be secured and processes automated for more trusted functionality, industry standard management and configuration of your encryption key management relies on human
management and must be straightforward, reliable, and easy to implement. A task-designed user-interface (UI) based off of observational preferences, time-on-task, frequency-of-task, number of users, and varieties of UI testing ensures greater intuition to complete tasks. This process is known as human-centered design, and is critical even for security systems to ensure proper configuration, management, and changes applied as intended.

**Documentation and FAQs**
Your key manager and extensible encryption mechanism needs to have adequate documentation and technical instructions readily available and up-to-date so that the organization is not required to produce their own. Professional documentation is evident through application and extensiveness of content and style guides to reduce reliance on vendor professional services and technical support through richer error messages, problem determination tools, and online FAQs available to the organization to eliminate vendor support calls.

**Affordability and Hidden Costs**
An enterprise should not need to license every end point that connects to the key server. The cost and complexity of licensing all endpoints is unnecessary and can be a huge barrier to getting data protection up and running quickly across the organization. Some vendors charge as much as $15,000.00 and more per connection. These hidden costs quickly add up and make a once thought-of cost effective solution an exorbitant expenditure within their environment.

**Transparency**
As part of establishing a relationship with your key management vendor, determine the transparency in providing information to an organization. For example, experienced security professionals require knowledge of customer identified defects that may also impact the security of their implementation. Seek a vendor that will share with you customer-reported bugs for the severity, duration to fix, and determination of secure coding practices.

**Conclusion**
These components of encryption key management are critical to determine the caliber of effective data security and the enduring success of your organization’s confidentiality, privacy, and brand name. As more enterprises begin to outsource hosting and move confidential data to the cloud, the protection of encryption keys becomes the number one action that determines the true effectiveness of encryption. Encryption key management based on FIPS compliant technology is the linchpin in a comprehensive and successful data security strategy. Key Management arms enterprises with stronger, defense-in-depth security that aligns with efforts to lower operational costs, meet compliance requirements, and accelerate deployment of mission critical security technology.

For more information regarding encryption key management must-haves in the cloud and the Townsend Security Alliance Key Manager (AKM), please reference:

- **eBook**: [Encryption Key Management Simplified](#)
- **Resources Kit**: [Encryption Key Management](#)
- **Video**: [Why is Unprotected Data a Business Problem?](#)
- **Blogs**: [Encryption Key Management](#)
- **Web Page**: [Alliance Key Manager](#)

---

**About the Author**
Joan Ross is the Chief Executive Officer at CISO Advisory Services and holds numerous security certifications including the NSA IAM, NSA IEM, CISSP-ISSAP, HISP, and FTK. She participates and presents at a number of cyber security, key management, and encryption conferences and seminars.

---

**Townsend Security**
Townsend Security creates data privacy solutions that help organizations meet evolving compliance requirements and mitigate the risk of data breaches and cyber-attacks. Over 3,000 companies worldwide trust Townsend Security’s NIST and FIPS 140-2 compliant solutions to meet the encryption and key management requirements in PCI DSS, HIPAA/HITECH, FISMA, GLBA/FFIEC, SOX, and other regulatory compliance requirements.

You can contact Townsend Security for an initial consultation at the following locations:

- **Web**: [www.townsendsecurity.com](http://www.townsendsecurity.com)
- **Phone**: (800) 357-1019 or (360) 359-4400
- **International**: +1 360 359 4400
- **Email**: info@townsendsecurity.com