

I D C E X E C U T I V E B R I E F

Making Key Management Work

October 2007

Adapted from *Data Protection Study: Data Encryption Option* by Charles Kolodgy and Brian Burke,
IDC #207606

Sponsored by nCipher

Introduction

Encryption is the linchpin of information security, yet most people don't think much about it. People expect the Internet to be secure, and they don't care about how that security is accomplished. That said, those who are responsible for protecting information and privacy understand what technologies are required, and encryption is one of those technologies. Enterprises have been deploying encryption in a piecemeal manner to meet specific needs, but the time is coming when they need to consolidate those encryption silos with a comprehensive enterprise key management system (EKMS).

This Executive Brief discusses the need for encryption and some of the developments around the technology, but the core discussion focuses on the value provided by a comprehensive EKMS. To help enterprises understand the developments around EKMS, we present user perceptions about encryption and key management, along with features associated with successful EKMS utilization. Some of the characteristics of a strong EKMS that are discussed in more detail are the following:

- Enables consistent enforcement of encryption policies and procedures
- Is able to scale to multiple encryption systems or applications
- Provides robust protection of the keys
- Offers automated and reliable recovery of encrypted data and keys

The paper concludes with IDC's take on what enterprises need to do to prepare for the future.

The World of Encryption

Cryptography and encryption invoke thoughts of mad mathematicians, spies, and paranoids. The reality is that encryption is the linchpin of information security. It provides the confidentiality and integrity required to protect information exchanged and stored by information systems. It is used by everyone nearly every day, and it is just done in the background so the average user isn't aware it is happening. Encryption's primary deployment is to protect communications ("data in motion") via virtual private networks (VPNs) or Secure Sockets Layer (SSL). At this level, encryption is used for transient data, and its encryption key life cycle is a short one.

The use of encryption has been expanding beyond the protection of communications channels to the protection of "data at rest." This expansion hasn't been undertaken for fuzzy reasons; there are hard and fast mandates supporting the growth in encryption. Two trends are fueling the encryption explosion — the proliferation of valuable digital data and regulatory mandates.

Why Encrypt?

The simple answer to "Why encrypt?" is to safeguard information from unauthorized access. Data is the lifeblood of the information age. For many companies, the information residing within their data systems — bits of information — is much more valuable than the atoms of physical assets. The value of information is manifested in the competitive advantage it provides; therefore, if the information is lost or stolen, there could be considerable ramifications. For example, in July 2007 a Boeing employee was arrested for having allegedly stolen 320,000 pages of proprietary digital data that the company claimed would have been worth billions of dollars to competitors. Earlier in the year, a DuPont scientist pled guilty to stealing 22,000 sensitive documents estimated at \$400 million.

In addition to proprietary data, considerable personal data resides in data systems. When personal information is lost or stolen, companies face a public relations nightmare and considerable penalties. In an IDC survey that asked IT professionals to rate the significance of factors driving the deployment of encryption, the top response was to "safeguard client or customer information," with 70% of the respondents saying it was extremely significant.

One reason for this need to protect client and customer information is that many government regulations mandate that specific types of information be protected from unauthorized disclosure. There are penalties for the exposure of this information and even for noncompliance with the regulations. Well-established government and industry regulations include Sarbanes-Oxley (SarBox), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley (GLB), state breach notification laws represented by CA-1386, and the Payment Card Industry Data Security Standard (PCI DSS). A few of the regulations specifically call out encryption as the approved method for protection; even for those that don't, encryption is considered the best way to protect the information.

Market Drivers

Organizations are taking the need to protect critical information, both regulated and nonregulated, seriously. Data-at-rest encryption is growing in popularity. Organizations that have been doing encryption are expanding its use to include more applications and more data, while organizations that haven't been encrypting are investigating and rolling out solutions. Various IDC surveys show that a third of all enterprises have some data encryption capabilities. Most organizations are either planning on expanding their present level of encryption or beginning to perform data encryption.

In a 2007 IDC survey, 75% of respondents said they expected their organizations' use of encryption to increase. An IT manager for a mining company summed up the firm's position regarding encryption this way: "Currently, we actually use encryption in very spotty fashion ... We could probably make a good case for doing a whole lot more ... We do so because the threats grow in capability and abilities so vigilance has to be constantly ramped up, and at some point we will probably encrypt everything just as another measure to protect ourselves."

The problem with this proliferation of encryption is that information systems have become ubiquitous — data resides in many different systems that require multiple encryption systems. All of these systems have their own approach to encryption, with their own key management system, which adds its own complexity, inconsistencies, and costs, but also makes it very difficult to share encrypted data across these applications and to provide the protection the keys require.

The problem for enterprises is complicated even more when they are bombarded by vendors selling backup encryption, storage encryption, file/folder and disk encryption, database encryption, email encryption, and some form of encryption for nearly every other data application. All of these products require the same things to make encryption work — data to be encrypted or decrypted, a cryptographic algorithm, and a cryptographic key. The last component is the most troublesome.

Value of EKMS

Data security relies on encryption, but within encryption, the linchpin is key management. At a basic level, key management systems provide secure life-cycle administration of cryptographic keys so that they are available where and when they are required. The KMS handles the secure generation of keys, recording key-related information, pushing keys to specific targets, auditing key usage, archiving keys for recovery of data, and ultimately destroying keying material when no longer required. Characteristics for basic key management include the following:

- Cryptographic policy enforcement
- Key creation

- Key distribution
- Key archiving
- Audit

These key management functions shouldn't be too daunting, and generally they are not, provided you have only one encryption application. The problem is that for proper privacy, security, and regulatory compliance, enterprises require multiple applications with encryption. Right now, each application uses its own key management schema, which creates considerable management and communications problems. This situation is on a course to get worse. As the need to encrypt grows, so will the number of applications requiring keys. The ultimate solution to this problem will be an EKMS.

An EKMS is a central key management system that unifies disparate key management policies and enables keys to be mobile across different endpoints or applications — an essential capability if data is going to move between these systems in an encrypted form.

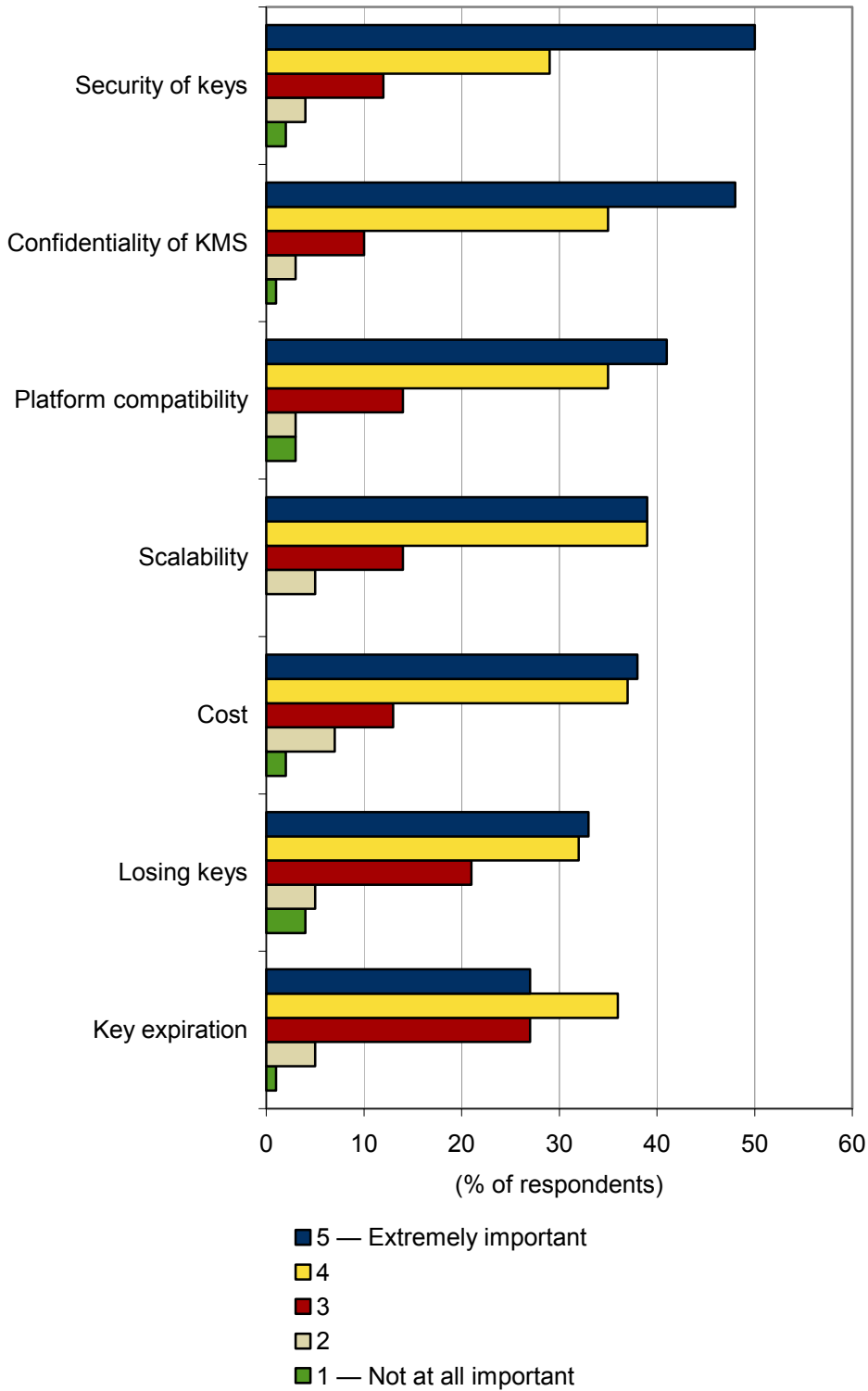
The characteristics of a general EKMS are very similar to those of any KMS, but some are unique to the EKMS. These variations include:

- Creation and enforcement of a central encryption policy
- Ability to manage a range of endpoints and applications
- Number of tasks automated
- Resilience and security of the EKMS

As Figure 1 shows, the top concerns associated with key management are the security of keys and the confidentiality of the KMS. If your keys are exposed, all of your encrypted data could be compromised. An insecure KMS means that you will not have a secure encryption solution.

Figure 1

Key Management Concerns



Source: IDC, 2007

The need for secure key management is always a concern, but if you have multiple encryption applications, each with its own key management system, you must secure all of the multiple key management systems and repositories. It is much more difficult and costly to defend multiple points than a single key management system. This single system would appear to be a single point of risk, but the cost and scrutiny required for a very secure single system offer considerable benefits over multiple risk points.

A central KMS removes some of that complexity and helps in securing all of an enterprise's keys. However, convenience isn't without its own problems. With a central key repository, if the keys aren't secure, you could lose all your data, not just what resides within one application.

The best way to mitigate the key management risk is to use hardware-based key management systems. These hardware key management platforms are designed to create an especially secure environment for the creation, dissemination, and storage of keys. It needs to be understood that the level of protection of your key management system must be at least equal to the highest level of protection of encrypted data. Ultimately, the KMS should be considerably stronger than the data protected by the keys.

Considerations: On Key Management Realities and Perceptions

In survey after survey, there is one constant barrier to the widespread deployment of robust data encryption: the fear that encrypted data cannot be recovered. When asked to rate the importance of data recovery when considering the use/deployment of encryption products, 49% of respondents said it was critical. Only reliability had a higher score. When respondents were asked about critical encryption features, key recovery/confidence of recovery was again second only to reliability, with 47% of respondents rating this factor critical.

Interviews with IT professionals put these feelings into words. IDC constantly hears some level of fear regarding the ability to recover encrypted data. One example is the following succinct sentence: "If you forget the key, you are toast." Another statement provides another view: "I was going to give the two main fears we have as complications of key management and not being able to recover data. Those are exactly the problems. ... This is a really dangerous technology in that encryption is a really good way to destroy data as well as protect it."

IDC believes that as more users experience enterprise key management — as they see it performing the functions highlighted in this document and not just handing out keying material — their fears will be eased but may never be totally erased. Users will eventually understand that a key management system requires automation, robustness, and reliability to perform all operations associated with encryption, from enforcing corporate policy to adequately protecting the data by performing the encryption and enabling the decryption of information when required.

IDC Analysis

Encryption and key management are hot topics. There is little dispute that the need exists and budget is being allocated. Nevertheless, considerable trepidation remains associated with the technology. As illustrated earlier, users have considerable concerns about the reliable recovery of encrypted data, and these concerns must be addressed for expanded deployment. IDC believes that vendors are doing well at the technology level but that there is still work to be done at the perception level. IDC feels this concern is partially based on a disconnect in perception.

Encryption and key management vendors correctly assert that the technology is mature and stable, but many users believe it is an unreliable or dangerous technology. The nature of the technology itself is partly to blame. Most people can understand that it is relatively easy to take readable text and convert it into unintelligible gobbledygook, but it is much harder to fathom that the unreadable data can be converted back into its original form. For this reason, data encryption is warily viewed as "black magic."

To get past these perceptions, vendors have turned to emphasizing the capabilities and robustness of key management. This is well and good, but many users, like a municipal public works utility systems programmer who said, "I'm going to be reviewing every resource that I can to determine who best effectively manages key management in a way that is compliant and gives me some sense of assuredness of that key being available. I want to mitigate that shuddering fear," are much less interested in the particulars of the key management system. Users are more concerned about the functions performed by key management and less concerned with the system's operations.

This is why survey data shows a much higher concern for the ability to recover encrypted traffic than for the specifics of the key management system. However, IDC believes the two should be considered together. Without a manageable, robust, secure, and reliable key management system, it is nearly impossible to ensure data and key recovery.

IDC believes that vendors must establish how their key management solutions directly address user fears associated with the recovery of data. Key management is important to decide what to buy, but people will buy only when they are confident that keys will exist to decrypt encrypted data. In this vein, the key management consideration isn't about technology; it is about results. One interesting item from IDC research is that some end users are going so far as to print out keys and store that paper in a vault so that they feel some level of control that they have physical access to the key.

Vendors need to understand how concerned people are about data recovery. If the customer decides that the key management system that is part of an application or KMS supplied by a third party doesn't provide a proper level of assurance of recovery and security, then the customer won't use it and probably won't use the encryption capabilities. IDC believes that organizations are most interested in purchasing key management solutions that are proven to work, and they will ultimately search for solutions that can manage multiple encryption applications.

IDC also believes that enterprises that have concerns about the security, reliability, and robustness of encryption and key management technology should turn to dedicated security vendors that have "been around the block" building and refining their encryption and key management offerings. Vendors dedicated to encryption for years, such as nCipher, which has been totally focused on enterprise encryption since 1996, have a firm grasp on the technology and have exhibited the level of commitment to the technology to inspire confidence in its robustness and reliability.

Conclusion

The information explosion has created an environment that requires data encryption. Digital data will continue to proliferate, it will grow in value, more people will need access to data, and privacy regulations will require more protection of that data. Given these facts, IDC believes enterprises must go beyond just performing encryption, they must develop a comprehensive encryption program that unites policy and enterprise key management with encryption applications.

It is possible to meet encryption needs with standalone siloed products, but as these individual components proliferate, the complexity, costs, and insecurity associated with multiple key management systems will arise. Instead enterprises must look at EKMS as a tool to be used across the enterprise. Although many encryption products are not presently able to use external key management systems, it's up to enterprises to plan for this inevitability, to push vendors for more open encryption, and to reward those forward-thinking vendors by offering API capabilities to allow the use of central EKMS.

Enterprises should buy for today but plan for tomorrow. That is, they should select a key management vendor and a product that not only can meet their immediate need but also will allow them to expand that key management offering into the future.

The time is now to investigate what the dedicated key management vendors, such as nCipher, are offering regarding centralized EKMS. IDC believes that developing a comprehensive encryption and key management program will enable improved security, ultimately reduce complexity, and be cost-effective. A comprehensive solution that makes it easier to deploy robust encryption globally will increase the comfort level to enable enterprises to expand the use of encryption within their information infrastructures.

In IDC's encryption survey, those thoughts were supported when 52% of respondents said they would be more inclined to deploy multiple encryption solutions if all components, including key management, could be managed under one console. Ultimately, the key is comprehensive encryption key management.

COPYRIGHT NOTICE

The analyst opinion, analysis, and research results presented in this IDC Executive Brief are drawn directly from the more detailed studies published in IDC Continuous Intelligence Services. Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. Contact IDC Go-to-Market Services at gms@idc.com or the GMS information line at 508-988-7610 to request permission to quote or source IDC or for more information on IDC Executive Briefs. Visit www.idc.com to learn more about IDC subscription and consulting services or www.idc.com/gms to learn more about IDC Go-to-Market Services.

Copyright 2007 IDC. Reproduction is forbidden unless authorized.