Security for Data at Rest: Critical Challenges and IBM Information Infrastructure Solutions

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Prepared for IBM

September 2008

Table of Contents

Executive Summary

The management of information risk has become one of the highest priorities of today's enterprise. Availability continues to be a primary objective of information management, but the definition and scope of availability has expanded to address issues from disaster recovery and business continuity to data retention. Retention requirements have themselves been stretched by a seemingly unending wave of regulatory compliance mandates, which also demand a higher standard of information protection against data privacy breaches and security threats that directly target sensitive information as never before.

Availability continues to be a primary objective of information management, but the definition and scope of availability has expanded to address issues from disaster recovery and business continuity to data retention.

The management of information in data center storage has become a focal point for all these concerns, which in turn has renewed interest in encryption for data at rest to assure these critical priorities. Encryption can secure data on storage devices when the devices leave the owners' control—such as when devices are repurposed, lost, or returned for an expired lease, repair, or for warranty replacement. It can protect data from unauthorized or unintentional discovery, lowering risks of exposure while preserving retention requirements and assuring information security and compliance.

Encryption cannot ever be deployed lightly, however. For a storage encryption strategy to succeed, it must answer several critical questions likely to be raised by storage and security professionals alike:

- Can information availability be assured against the effective loss of data due to poorly managed encryption or the loss or damage of decryption keys?
- Can keys be both adequately secured and adequately available without exposing the entire strategy to risk?
- Can the cost and performance impact of encryption be reduced or eliminated?
- Can it assure security without further complicating already complex storage and data center environments?

Recent developments in self-encrypting disk and tape drives offer a number of positive answers to these questions. In concert with an approach to cryptographic key management built on long experience, the data center today has more options for deploying secure, transparent and low-impact encryption for data at rest than ever before.

These options must, however, be deployed in concert with a comprehensive approach to information availability, retention, compliance and other security policies. They must be integrated with best practices in encryption and key management—a domain where expertise can have a greater impact on a successful deployment than few others in IT.

As part of its Information Infrastructure approach, IBM is today embracing these challenges with new solutions for assuring cryptographic security in data center storage. In this paper, Enterprise Management Associates (EMA) takes a closer look at these IBM solutions, which combine self-encrypting disk and tape offerings with a key lifecycle management approach based on proven solutions and a newly-expanded vision. Executives will gain a new

appreciation for the comprehensive range of IBM information security solutions that can help customers of all sizes protect their most valuable information assets.

Information risk management has always been a high priority for the enterprise, but in recent years, the time-honored requirements to assure information confidentiality, integrity and availability have undergone a radical transformation.

Information Risk Management: Today's Challenges

Information risk management has always been a high priority for the enterprise, but in recent years, the time-honored requirements to assure information confidentiality, integrity and availability have undergone a radical transformation.

From managing day-to-day operations to safeguarding intellectual property on which the viability of the business itself may depend, **availability** remains the cornerstone of information assurance. Information availability is directly related to IT resource performance, and is one of the highest priorities for assuring agile, responsive IT. Today, however, with increased focus on issues from disaster recovery and business continuity planning to document retention, availability has taken on an even broader meaning. Beyond primary information storage and management resources, availability management extends to backup and recovery, offline and "nearline" storage. This raises the bar on information protection: how can the business assure information confidentiality as well as integrity in all these cases—particularly when the business may not have the most direct control over its own information, as when it may be stored offline at distant facilities or in the care of third parties?

The need to protect sensitive information has become even more urgent in light of **security** threats that have exploded in recent years. Stolen or exploited personal information now has tangible value, particularly to organized criminals that increasingly dominate the threat landscape, and for good reason: personal information is often directly linked to tangible assets. According to the Privacy Rights Clearinghouse, more than 200 million personal records of U.S. residents have been exposed since January 2005[1]. Stock values of some public companies have declined as much as 17% within the first 15 business days following the disclosure of a data security breach, and some such as CardSystems have been all but forced out of business as a result.

All these factors have produced more intense regulatory **compliance** demands for information risk management than ever before. Today, the majority of U.S. states, a number of countries, and even entire business segments, such as retail, have adopted some form of data privacy regulation. Forty-three US states so far have enacted data privacy laws providing a safe harbor from data breach disclosure if organizations can show that lost or stolen data was encrypted. The Payment Card Industry (PCI) Data Security Standard goes into an unprecedented level of detail in mandating controls on information risk, while measures such as the Federal Rules of Civil Procedure (FRCP) define specific requirements for data **retention** to which virtually every entity under jurisdiction must comply.

[1] http://privacyrights.org

These challenges often place demands on business that may be considered paradoxical at best, if not actually contradictory at worst. Data retention and requirements for availability assurance, for example, often require information to be stored for long periods, in both online as well as offline or near-online forms. This long retention, however, exposes information to risks of unwanted discovery or exploit. How can businesses balance all these conflicting demands?

A Renewed Focus on Encryption…but with a Caveat

All these factors are bringing a renewed focus on addressing these issues with encryption of data at rest. It can assure that storage media do not inadvertently expose sensitive data when tapes or disks are removed from service and archived internally or delivered to third parties for management—or lost.

There are, however, some very big "ifs" when it comes to managing the encryption of data at rest with confidence. The deployment of encryption can have a direct and potentially critical impact on the management of storage and information systems themselves. Security professionals must understand these issues in order to win the confidence of storage managers in a successful deployment. On the other hand, encryption is often seen as a domain requiring sophisticated security expertise, which may intimidate even knowledgeable storage professionals. While storage professionals need not become security experts to safely deploy encryption, there are some essential factors they must bear in mind for encryption to be truly effective.

Deploying Encryption: What Security Professionals Should Know About Storage…

Storage professionals will want to know that security teams understand their concerns and are prepared to address them in a mutually supportive way. Issues they may raise might include the following:

Keeping business-critical applications available is an imperative that must also be assured in the event of data loss, regardless of the reason. This means that encryption management must also factor into areas from backup and recovery strategies to disaster recovery and business continuity planning.

"I can't afford to lose data because of poorly managed encryption. Can you assure me that my data will be available?"

One does not have to be an expert in cryptography to understand that lost keys required to decrypt the data leads to unrecoverable data. Cryptographic key management will therefore be one of the storage manager's top concerns. Beyond this fundamental issue, however, are requirements for assuring availability and performance according to service levels and policy demands.

Keeping business-critical applications available is an imperative that must also be assured in the event of data loss, regardless of the reason. This means that encryption management must also factor into areas from backup and recovery strategies to disaster recovery and business continuity planning.

Business partners, customers, and other authorized third parties often require access to data—even though it may be encrypted. This calls for flexible and effective key management to ensure that third parties across the extended enterprise will have the appropriate access to the firm's information.

"I can't afford to have encryption negatively impact performance"

The potential performance impact of encryption is not a minor issue. Since each cryptographic operation is essentially a mathematical calculation involving very large numbers, the computational impact is considerable. Performance is more than an operational concern, however. When planning a data recovery strategy, for example, data must be recoverable *to* a specific point in time (Recovery Point Objective or RPO) as well as *within* a specified time (Recovery Time Objective or RTO). Encryption cannot impact these objectives beyond tolerances defined by the business.

Security professionals will go far in assuring storage managers that they understand these concerns by embracing techniques that improve the performance and reliability of an encryption solution. For example, moving encryption operations closer to the storage media can reduce the potential for performance bottlenecks in the datapath, since the various storage drives are doing encryption in parallel at native drive speeds. These factors can benefit the performance of both storage *and* encryption operations and help assure that application service level objectives are being maintained.

If not integrated well, encryption can complicate an already complex storage environment, as well as the applications that depend directly on the availability and performance of the storage environment.

"How will encryption further complicate my environment?"

If not integrated well, encryption can complicate an already complex storage environment, as well as the applications that depend directly on the availability and performance of the storage environment.

While security professionals recognize that increasing complexity can increase risks, as well as increase costs, they may not fully understand the impact of security on idiosyncratic network-attached storage (NAS) environments, which include network and storage devices, as well as servers that must be well-coordinated for optimal performance and minimal risk. Encryption that exacerbates this complexity may place both storage *and* security priorities at risk. A solution that is more transparent to these complex environments can reduce the total impact of encryption and improve the manageability of storage as well as security.

"How can I control my costs if encryption becomes a requirement?"

All these factors—availability, performance, and complexity—can substantially increase storage management costs when encryption is introduced, while the cost of encryption solutions themselves must be weighed against their benefits. To address these legitimate storage management concerns, security professionals must gain a better understanding of different encryption and key management models that minimize or eliminate availability,

performance, and complexity risks, as well as understand and assess the suitability of products that include cryptographic functions as an option to their traditional offerings.

What Storage Pros Should Know About Security

Just as there are aspects of storage management that security professionals must understand, storage professionals need to understand certain fundamentals of security in order to successfully deploy an encryption solution and avoid misplaced confidence in an inadequate deployment.

Imperative: Keep Keys Secure

Encrypted data is only as secure as the keys used to authenticate, encrypt and—more importantly—to decrypt or "unlock" data. The security of these keys is, therefore, paramount, and storage professionals must recognize that steps must be taken to ensure both the availability and security of these keys. Careful planning in this regard is essential. Lost or exposed keys can compromise the security of the data they are supposed to protect. To that end, effective key management must accommodate a variety of risks, use cases, application security, and related IT management systems. Assuring secure and reliable key management is one of the most critical factors that can make or break a successful deployment.

Imperative: Keep Keys Available

Security professionals recognize that key availability is essential to the availability of the data itself. For storage professionals, however, high availability requires redundant copies of critical information, and while cryptographic keys are indeed critical information, precautions must be taken to ensure backup copies are also secure to mitigate risk to any copies.

The availability of keys in real-time operations is even more critical. One might think that this is a typical if not critical requirement of key management, but storage professionals may be surprised to learn that serving keys to the appropriate systems, applications and services is not always an integral feature of a key management product. Storage professionals and their security counterparts should collaborate to assure that these capabilities are part of real-time key management performance.

Today's Choices for Encryption of Data at Rest

These factors should be considered in light of today's choices for the encryption of data at rest:

In Applications

Application-based encryption can be effective in securing small portions of data, such as individual fields within a database. This adds a layer of security that is more appropriate for Web applications or databases where end users typically have restricted views of data fields. Application-based encryption is software-based encryption, which often has a meaningful impact on the performance of the application server upon which the encrypting application resides. While the amount of data selected to be encrypted is limited, organizations must be certain that they have encrypted *all* items necessary. The challenge with this is that databases can be fairly fluid and may undergo periodic, if not frequent, changes in content and design. As new fields are added or changed, regular assessments must be done to assure

that the appropriate fields are still protected. This is not a "set it and forget it" model, and the organization is reliant on its database administrators to manage this effectively. Aside from the impact on application management, these factors could also have a downstream impact on dependent applications, as well as a performance impact on the application server. Because application-based encryption typically addresses a limited set of data, it is not the preferred method for efficiently protecting the data on storage devices that are eventually physically removed from storage systems.

In the SAN

A distinction must be made between the encryption of data in motion, where it moves through a network, and encryption of data at rest, where it is encrypted on the storage media. Session encryption is typically used in the former case to protect data as it moves across public and private networks beyond the physical security of the data center. Since the exposure of the ciphertext (encrypted data) is very brief as the data travels across the network, encryption keys are typically short-lived and relatively short in length. To protect data at rest, however, organizations need stronger encryption methods that are more appropriate for long-term data storage. Here is where you see longer, persistent encryption keys. Both options expose the encrypted text which can be used to "crack" an encryption key, so it is imperative that organizations match the right model to their needs. Deploying centralized encryption appliances in the SAN may also pose risks of performance bottlenecks, as well as single points of failure that threaten data availability. This could risk data availability for a given session, as well as long-term availability if the failure destroys access to encrypted data at rest.

In General

Overall, most of today's approaches to data encryption add significant complexity and cost with a variety of elements required to adequately secure data. One of the most common—and most difficult—challenges of many approaches is that they require the careful classification of sensitive information in order to minimize unnecessary costs. Data classification has long been touted as a best practice in information security—but it is also one of the most difficult objectives to achieve realistically, with true accuracy and reliability. These issues highlight one of the paradoxes of encryption: some of its greatest barriers to success often have little if anything to do with the technology of cryptography itself.

Overall, most of today's approaches to data encryption add significant complexity and cost with a variety of elements required to adequately secure data.

When encryption is implemented in software, organizations must recognize that cryptography can be highly CPU intensive. As described earlier, these factors can impact application performance and may require additional processing power to support the added workload. Modifications such as hardware accelerators on host bus adapters can help overcome these factors, but they may also necessitate additional upgrades in the data path, or even the reconfiguration of critical applications. Emerging encryption standards may also require that multiple keys be used, which complicates the planning and deployment of key management. Moving encryption to the "back side" of a storage system rather than in the front-end application or the SAN may not substantially change these factors.

A Critical Question

A critical question that any encryption initiative must answer is this: Does the approach adequately resolve the risks it was intended to address?

A critical question that any encryption initiative must answer is this: Does the approach adequately resolve the risks it was intended to address?

If it requires data classification, any gaps in the planning or actual effectiveness of the classification strategy may undermine the solution. This is an even more serious issue when data is stored offline, as with tape. Enterprises must be assured that their data has been fully protected against loss or theft of the media itself.

While lost tapes have made headlines, offline disks pose very similar issues that may be even more serious, considering the increasing capacity of today's disk drives. Disks have a finite lifespan and are retired from service for many reasons. For instance, individual disks might be failing and need to be replaced under warranty. Enterprise disk systems are also occasionally repurposed internally, returned at the end of a lease, or sold to a third party. And, of course, disk drives can also be lost or stolen, either individually or as part of a system. Even disks that are RAID protected do not adequately protect the business against exposure, simply because they distribute data across multiple disks. The sheer size of modern drives alone makes it highly probable that useful data can be retrieved from a typical RAID stripe.

To assess these risks of data exposure, IBM performed a study of failed disks returned under warranty and found that as many as 90% still contained readable data. Considering that, in IBM's estimate, as many as 50,000 disks are retired from data centers every day, the potential for sensitive data exposure may be much higher than many suspect.

The Advantages of Drive Encryption

When well implemented, drive-level encryption can protect against many of these issues, including security for offline storage. It can reduce or eliminate data classification requirements, because *all* data can be encrypted directly in storage media. It can alleviate performance concerns by embedding the encryption engine directly into the individual drives. What's more, encryption performance scales linearly as each drive includes its own encryption engine. When deployed within highly available storage environments, the benefits of simple deployment and ongoing management are difficult to match.

Furthermore, today's self-encrypting tape and disk drives can deliver these benefits with a high degree of transparency to applications and application servers, as well as to storage systems themselves. They must, however, be accompanied by effective storage management and key management policies to deliver on their full potential.

IBM: Answering the Challenge

The values of drive encryption—for disk as well as for tape—are at the heart of IBM's approach to security of data at rest, for assuring transparent yet comprehensive security as well as significant performance advantages. Though foundational, this is just one part of the comprehensive IBM Information Infrastructure (III) approach to assuring end-to-end data compliance, availability, retention and security priorities. As a leader in mainframe

computing, IBM has long recognized the values the high-assurance mainframe environment brings to an encryption initiative. The company also offers a range of flexible approaches to cryptographic key management, to assure that the confidence placed in encryption is well founded. When complemented by the Tivoli family of leading identity and access management solutions, the recognized security expertise of IBM Internet Security Systems, and highly experienced services for security and compliance assessments and outsourcing as well as implementing information risk management, the IBM Information Infrastructure approach offers a comprehensive enterprise portfolio of solutions for securing sensitive information.

Encryption at the Drive: Leveraging the Advantages of Self-Encrypting Disks

With recent advances in disk encryption integrated directly in the drive, self-encrypting disk drives pioneered by key IBM partner, Seagate, equips modern storage systems with security for data-at-rest that is essentially transparent to business-critical applications and platforms.

Self-encrypting drives encrypt and decrypt data on the disk using an encryption key embedded in the drive itself. This key can itself be encrypted using a separate authentication key maintained by an enterprise key management system, to assure that only authenticated parties can access the data on the disk. The encryption key, encrypted with the authentication key, is only stored on the drive in this secure format and is only decrypted for use in the drive's silicon to encrypt and decrypt data after access to the drive is authenticated. Should the drive be physically removed from the system, the drive would be "locked" until it is again inserted in the storage system and subsequently authenticated again with the key management system. Without this power-up authentication, the encryption key would be inaccessible—as would the encrypted data stored on the drive. The encryption key never leaves the drive, yet it can be changed by the drive owner to eliminate the risk of a warehouse attack (an attack based on a knowledge of the key with which the drive was delivered).

This drive-level approach enables transparent encryption and decryption of data only when data is read from and written to the disk. The data stored on the disk remains encrypted at all times. This approach makes encryption more straightforward to deploy and manage. It introduces little to no performance degradation since the entire encryption operation is distributed across all disks in the system in parallel, rather than through a single encryption engine or appliance. What's more, the embedded encryption engine is an ASIC that automatically matches the speed of the device port, which enables encryption at native drive speeds.

Self-encrypting drives can also eliminate data classification requirements, which can address certain compliance mandates since they transparently encrypt all data written to the disk. They also greatly simplify the task of data destruction on decommissioned drives since the data is rendered inaccessible simply by changing the embedded encryption key. By doing so, users can immediately reuse the drive without fear of exposing the older data.

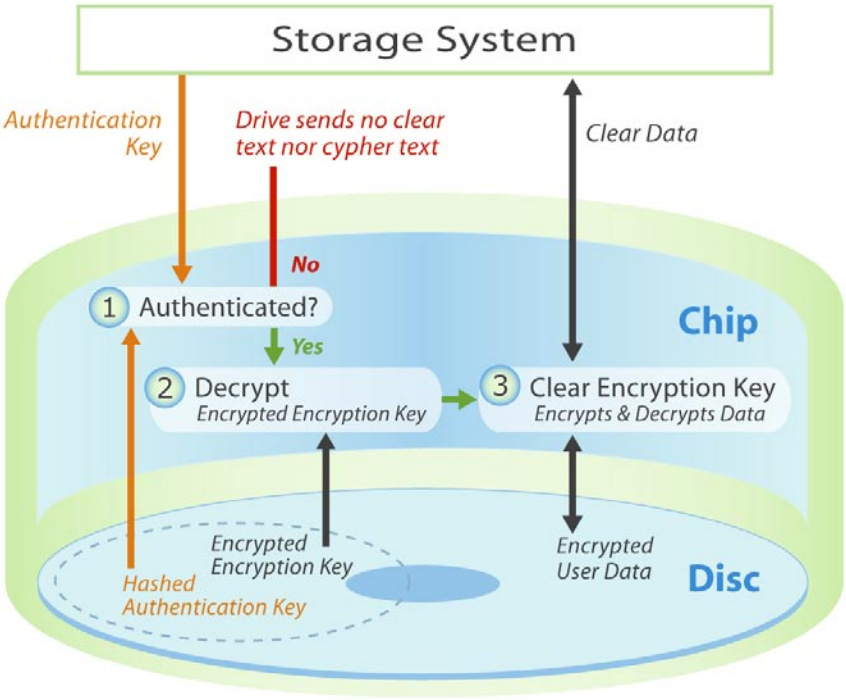

Figure 1: Self-encrypting disk drives offer superior protection of data at rest, with persistent encryption keys never leaving the drives

Because encryption operations take place on the disk itself, this approach also has little or no impact on end-to-end storage Protection Information (PI), or on data compression and de-duplication strategies critical to the performance and efficiency of the modern data center, as encryption occurs well after those operations. This compares favorably with approaches to encryption deployed farther upstream of data flows to and from storage, which can severely impact data compression, for example, since encrypted data is effectively uncompressible. This offers additional benefits to energy efficiency initiatives, which continue to be a priority in many data centers today.

Key management is also simplified since multiple keys for multiple disks need not be escrowed or otherwise backed up securely to assure data recovery—potentially an enormous burden. Only the authentication key and the disk drive itself are necessary to assure data access. Periodic re-keying is another common key management challenge. When encryption keys are exposed throughout the enterprise, periodic re-keying may be required to protect keys and the data they protect. Because the encryption is embedded in the drive and never leaves the drive, re-keying for these specific purposes is seldom necessary. When re-keying is required, it is done without decrypting and re-encrypting all the data. This can substantially reduce the need for what has traditionally been a very time consuming process.

Encryption at the Drive: Reaping the Full Benefits of Tape

Self-encrypting disk drives present a new range of options for significantly improving the management and effectiveness of encryption. Tape, however, continues to represent a substantial proportion of the information the enterprise must secure and control. For a tiered storage strategy, tape continues to make economic sense in many businesses. For offline or long-term storage, tape management continues to be a relatively straightforward and cost-effective option, particularly for archiving requirements that can extend to several years. Modern tape storage systems address performance and availability issues in ways that diminish the differences between online and "nearline" performance while preserving a significant portion of the TCO advantage of tape storage. Tape remains a preferred solution to these storage challenges among many enterprises

Resiliency is another reason for maintaining a tape storage strategy. Put simply: tape lasts. Disk systems often cannot stand up to the environmental stresses that tape can withstand—a key factor when data availability is critical. Tape may also be less subject to system-related issues such as security attacks against online data, or information lost or damaged due to application or system defects. These are all key factors when planning for disaster recovery or business continuity on which the enterprise itself may depend for its survival. Tape is therefore still seen by many as "the ultimate authority" when the resilience and integrity of data are critical. It is still, however, subject to all the risks of tape loss, theft or discovery that threaten security and compliance.

To address these information risks while preserving the ongoing value of tape storage, IBM has embedded encryption within its IBM System Storage TS1130 (formerly the TS1120) and Ultrium LTO Generation 4 tape drives. The aforementioned self-encrypting disk solution is modeled after IBM's self-encrypting tape solution, which has been available for over two years. IBM self-encrypting tape drives use one set of keys to encrypt and decrypt data on tape and additional keys to authenticate and protect access to encryption keys. Symmetric keys used to encrypt and decrypt data are written to write-only registers of the drive and are never exposed outside the drive. Once used, these keys are deleted from the drive itself. Asymmetric or public key cryptography is used both to authenticate the drive, as well as to encrypt data encryption keys in transit to or from the drive. This eases encryption management by abstracting controls on access to encryption from encryption capability itself.

Should access to encrypted tapes be required by a third party, an additional set of authentication keys can be employed, both to authenticate the third party as well as to secure data encryption keys. Use of these additional authentication keys are subject to the exclusive control of the information owner, however, which allows data to remain encrypted even when tapes are off-premises or in the hands of business partners, as well as when lost or stolen. Together, these benefits help to assure tape data security in a wide variety of use cases.

As with self-encrypting disks, encrypting tape drives can be deployed with high transparency to applications and business systems. In addition, they can eliminate interference with data compression and de-duplication initiatives critical to enhancing storage efficiency and reducing data center energy consumption. Not least of all, IBM encrypting tape drives offer cryptographic security as an added value, delivered with the drive itself at no additional cost.

Encryption on the Mainframe

The investment in mainframe computing continues to be one of the most viable in the enterprise. In addition to being a common platform for enterprise information management, the mainframe is still one of the highest-confidence environments in IT. As threats continue to proliferate, these factors have led to increased attention given to the role of the mainframe as a strong information security enabler.

IBM z-Series computing power combined with the reliability of mainframe access controls help support the use of the mainframe to directly encrypt data with high performance within the secure mainframe environment.

IBM Encryption Facility for z/OS allows businesses to leverage the values of mainframe computing in an encryption security strategy. IBM z-Series computing power combined with the reliability of mainframe access controls help support the use of the mainframe to directly encrypt data with high performance within the secure mainframe environment. This capability may be particularly valuable to the business that must exchange sensitive information with partners, since it can relieve the need to install any additional or special purpose hardware to support data encryption.

The IBM Encryption Facility for z/OS consists of two primary components: the Encryption Services feature for the mainframe platform, and the Encryption Facility for z/OS client. The Encryption Services feature supports encryption and decryption of certain z/OS file formats for archiving or transfer to business partners. Encryption is carried out prior to writing to disk as well as to tape or other removable media. The DFSMSdss Encryption feature additionally supports DFSMSdss dump data sets. Both support hardware-accelerated compression before encryption. Options that increase the range of IBM Encryption Facility for z/OS capabilities include the Encryption Facility for OpenPGP support, designed for compatibility with OpenPGP standard (RFC 2440) requirements.

Additional client-side functionalities expand the solution's usefulness. These include a Decryption Client for z/OS systems that supports decryption of data encrypted by the Encryption Facility system z format. While it cannot be used to encrypt data, the Decryption Client for z/OS gives businesses the ability to read, on one z/OS host, the data encrypted with the z/OS Encryption Facility on another, which can help improve information exchange processes.

An additional client option for Java-based systems supports both the encryption and decryption of z format data secured by the Encryption Facility for z/OS. Although the Java-based Client cannot process data created using compression, it does expand the range of platforms that can take advantage of the IBM Encryption Facility for z/OS to any Java-based system.

Essential to Strategy Assurance: Key Management

While encryption embedded within storage drives offers many advantages over other approaches, the reality of the modern enterprise is that there are many ways to encrypt data. Already, businesses routinely encrypt network communications using VPN technologies and Web or application traffic using SSL or TLS. Messaging infrastructures increasingly use cryptography to assure communication privacy and security. Cryptography is also used

to assure and validate access credentials with higher confidence, as with federated identity management, while encryption of data-at-rest extends to file and folder encryption on storage media. In all these approaches, one aspect in particular is paramount: the confidence placed in the keys that encrypt and decrypt sensitive information. An encryption strategy directly depends on this confidence.

Key management is therefore one of the most important aspects of an encryption strategy. Not only must it secure these many applications of encryption, it must also protect the sensitive phases of the cryptographic key lifecycle. It must provide for the secure and reliable generation of keys. It must manage the "lifespan" of keys, considering that keys may be retired due to risks of discovery and exploit. It must be able to respond to cases of key compromise, which places critical data sensitivity at risk. It must safely destroy keys when no longer needed, while simultaneously assuring secure and reliable backup contingencies in case of key loss.

A truly comprehensive key management system must securely place keys into production, and make them available to dependent systems and applications as transparently as possible—but only as needed, restricting all other access.

Many key management systems address these phases of the cryptographic key lifecycle, but there is one additional aspect that many do not. A truly comprehensive key management system must securely place keys into production, and make them available to dependent systems and applications as transparently as possible—but only as needed, restricting all other access. This requires a high degree of compatibility with many encrypting applications and systems, as well as with IT assets specific to key management, from configuration files to system specific "keyrings," file-based key stores, cryptographic devices, and so-called "hardware security modules" (HSMs) dedicated to securing high-sensitivity keys.

The IBM approach to key management revolves around IBM Tivoli Key Lifecycle Manager (TKLM), a product announced in 2008 that will be enhanced in phases. From an initial focus on key management for tape and disk encryption, IBM plans to expand TKLM into a centralized key management facility for managing encryption across a range of deployments.

Tivoli Key Lifecycle Manager represents the convergence of a number of key management drivers at IBM. One is the evolution of IBM's Encryption Key Manager (EKM), part of IBM's Java resources, which provides key lifecycle management and serves keys to encrypting drives in two ways. In a system-managed deployment, EKM provides key management services to z/OS, AIX and Solaris systems hosting encryption services. In a library-managed deployment, EKM provides key management services to an encryption-aware tape library, such as the IBM TS3400 and TS3500 series. In both cases, EKM provides key lifecycle management and serves keys to IBM TS1130 and LTO 4 encrypting tape drives. EKM itself can be hosted on the same platform with the environment it serves, or on a different server than the tape application, such as a dedicated host or high-confidence mainframe. (A third option, application-managed encryption, is represented by the key management capabilities of IBM Tivoli Storage Manager, which provides self-contained key services for attached encrypting drives.)

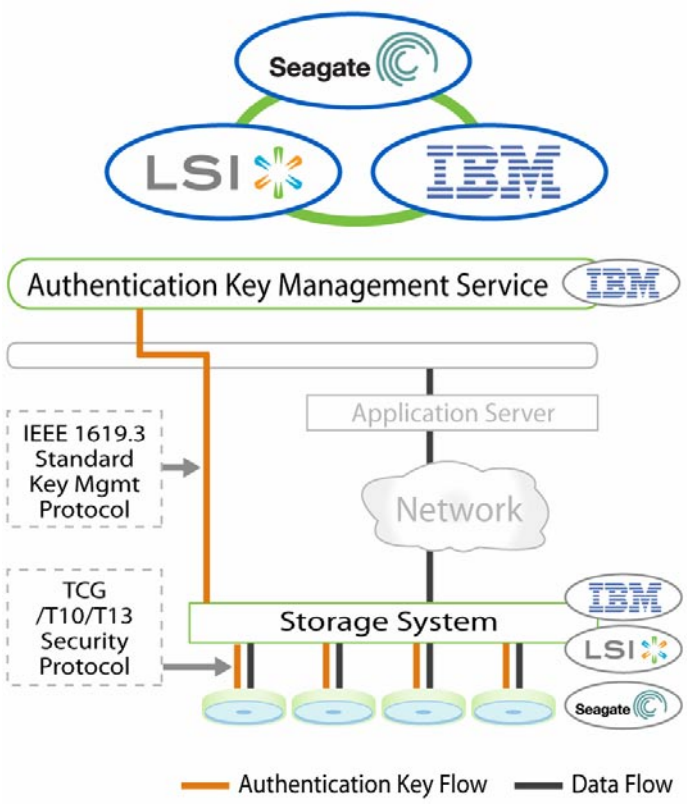

Figure 2: With its strategic partners, IBM provides key management as an essential and integral aspect of a comprehensive, standards-based data-at-rest encryption strategy.

Other major drivers of the emergence of IBM Tivoli Key Lifecycle Manager include the continued evolution of encrypting storage drives, and the increasing need for enterprises to take a more comprehensive approach to key management due to the increased deployment of encryption. TKLM will provide key lifecycle management and key serving to encrypting disk drives as well as to encrypting tape systems. It will provide role-based administration and capabilities for key archive and backup, the ability to refresh or replace expiring key certificates, enhanced reporting and audit as well as scalability, and will also provide a GUI for the administration of Enterprise Key Manager.

As TKLM capabilities expand in the coming months, it will additionally embrace traditional key management services such as digital certificate management, the ability to work with recognized certificate authorities (CAs) for external validation of cryptographic keys, and support for a number of security-employing applications and resources such as SSL servers. It will define and enforce security policies such as encryption algorithm and key length, and usage parameters encoded in key metadata. It will support well-established standards for implementation and interoperability of cryptography such as PKCS#11, as well as emerging standards such as IEEE P1619 and T10 for storage encryption, as these standards mature. It will target scalability in capabilities such as the large-scale import of keys from existing cryptography deployments, and provide a number of other services that support more comprehensive key management for the encryption-aware enterprise.

Beyond Data-at-Rest: IBM Information Infrastructure and Security Management Resources

Of course, securing sensitive information extends beyond encryption services for data-at-rest. Once retrieved from encrypted storage, information may be put in motion or in use "in the clear," in an unencrypted format. In order to be truly effective, encryption must therefore be a part of a larger initiative to assure the security of IT resources and sensitive information, wherever found.

IBM recognizes these realities and embraces them in an end-to-end approach to information security. Encryption for data-at-rest is just part of the IBM Information Infrastructure (III) initiative, which seeks to protect information wherever it is. The ability to secure sensitive applications is one of the primary objectives of the company's Rational group, augmented in recent months with acquisitions such as DataPower for enforcing security policy on integrated Web Services, as well as of Watchfire, a leading vendor of Web application security assessment and management products. IBM's Tivoli family includes market-leading resources for identity and access management central to security enforcement and regulatory compliance, as well as security event management and System z security management. With the acquisition of Internet Security Systems, IBM has become a leader in IT security products as well as security professional services. Augmented with recent large-scale data center buildouts to support much-desired capability for providing IT "in the cloud," IBM has taken one of the most comprehensive approaches in the industry to the assuring of the security of sensitive information, from storage to protection for data in motion and in use.

EMA Perspective

An encryption initiative can never be taken too lightly. Experience has proven that encryption and key management can be among the most challenging initiatives undertaken by the enterprise. It has also proven that nothing is as essential as experience for assuring success in these domains.

Today, technologies such as self-encrypting storage drives significantly reduce many of the challenges of encryption, making cryptographic security for data-at-rest more transparent, more manageable, and more cost-effective. As these values bring manageable encryption within the grasp of more enterprises, a policy of encrypting any or all data at rest in the data center becomes much more realistic. It certainly comes much closer to the positive security model of "deny all except" commonly encouraged as best practice in security, namely one that shuts the door on all risks and permits only those functions needed by the enterprise. Encryption must, however, be deployed with well-informed care in order to avoid placing the enterprise itself at risk.

IBM is one of the few vendors that can credibly leverage a long history in encryption, in the development of technologies as well as in a sizable body of experience in deployment. With what has become a dominant range of products and services for information security, IBM stands in a position few other major competitors can match when it comes to the breadth of capability it offers, now augmented by the ability to leverage the transparent efficiencies of encrypting drives and expanding key management capabilities for securing data at rest.

With what has become a dominant range of products and services for information security, IBM stands in a position few other major competitors can match when it comes to the breadth of capability it offers, now augmented by the ability to leverage the transparent efficiencies of encrypting drives and expanding key management capabilities for securing data at rest.

This is not to say that IBM has taken into its portfolio *all* the resources necessary to secure sensitive information in today's environment—but neither does it need to in order to succeed in its information security strategy. It partners with companies such as Seagate for self-encrypting disks and system vendors like LSI for designing some of its self-encrypting disk systems. It has strategic relationships with leaders in other domains such as network infrastructure for assuring the security of data in motion as well as at rest. And with a well-developed (and continuously evolving) approach to professional security services, it is able to embrace the heterogeneous reality of the modern enterprise, helping today's more risk-aware businesses address its most significant security and compliance concerns.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst and consulting firm dedicated to the IT management market. The firm provides IT vendors and enterprise IT professionals with objective insight into the real-world business value of long-established and emerging technologies, ranging from security, storage and IT Service Management (ITSM) to the Configuration Management Database (CMDB), virtualization and service-oriented architecture (SOA). Even with its rapid growth, EMA has never lost sight of the client, and continues to offer personalized support and convenient access to its analysts. For more information on the firm's extensive library of IT management research, free online IT Management Solutions Center and IT consulting offerings, visit www.enterprisemanagement.com.

Corporate Headquarters:
5777 Central Avenue, Suite 105
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com

1722.090408