IBM Security
Thought Leadership White Paper

August 2015

Encrypting data with confidence, across the enterprise and beyond

Reduce complexity, cost and risk by leveraging industry-standard encryption key management

IBM

Contents

Introduction

With ever-increasing security threats, mounting regulatory requirements and the explosive growth of data, effective data protection is more important than ever. Many organizations have turned to encryption to protect data at rest or in motion, using hardware, software, system components, network appliances and custom applications. But this fragmented approach has increased costs and complexity; imposed disparate processes for managing security policies, encryption keys and compliance reporting; increased the risk of data loss; and led to migration difficulties during upgrades needed to maintain platform currency.

Given the complexity of implementing encryption, IBM joined a consortium of vendors in defining a pragmatic, industry-standard approach for encryption—now known as the Key Management Interoperability Protocol (KMIP). With KMIP, organizations can now use interoperable, standards-based solutions to integrate encryption technologies and key management systems. KMIP is a simple "on-the-wire" protocol that has enabled organizations to deploy encryption and key management within a wide variety of industries. In fact, the latest revisions to the KMIP standard reflect these real-world implementations.

This white paper discusses an integrated approach for easily managing the lifecycle of encryption keys, based on the transparent use of built-in, hardware-assisted encryption and simple, standards-based key management. It also explains how organizations can feel more confident about encrypting mission-critical data across the enterprise, in the cloud and beyond.

The evolution of encryption

Today's organizations are faced with a constantly changing threat landscape in which sophisticated attackers and new attack technologies make it increasingly difficult to ensure the security of confidential data. One of the best ways to protect data is with encryption, and recent changes in encryption technology, regulatory requirements and deployment processes have led to organizations across diverse industries taking a new look at adopting enterprise-wide encryption.

Hardware changes

For a long time, encryption has been used in specific areas, often in financial and government sectors, where critical security needs could justify the cost and complexity of the methods available. Practical concerns had prevented wider adoption, and most organizations had shied away from encryption due to performance concerns and a lack of sufficient technology. The good news is that hardware acceleration, in which processors and devices have built-in technology for accelerating encryption, have removed the need to trade off performance for data security in many cases.

In addition to enabling encryption at wire speeds, the IT industry needed a key management and consumption approach that would allow applications and servers to read and write encrypted data transparently. With improved key management and usage, organizations would be able to deploy encrypted devices—such as storage devices—to protect data without impacting the rest of the infrastructure.

To meet this need, IBM introduced a feature in its storage arrays and tape libraries called transparent encryption that enables the reading and writing of data without any need to know about the encryption keys working behind the scenes. The storage device simply interacts with a key manager that supports its usage model when it needs keys. As a result, encryption occurs transparently, with almost no overhead to the organization, so administrators can easily implement data encryption since nothing else in the infrastructure has to change.

Regulatory expansion

While hardware advances have made the adoption of encryption easier than ever, the types and amount of data that need to be encrypted continue to increase.

Encryption is mandated by a variety of regulations and standards, such as the Payment Card Industry Data Security Standard (PCI DSS), the Federal Information Security Management Act (FISMA), the Sarbanes-Oxley Act (SOX), the Gramm-Leach-Bliley (GLB) Act, the Health Insurance Portability and Accountability Act (HIPAA), and the Health Information Technology for Economic and Clinical Health (HITECH) Act. International organizations such as the European Union and the Monetary Authority of Singapore have strict laws about data privacy, while in the US, individual states such as Massachusetts and Nevada also mandate encryption.

---

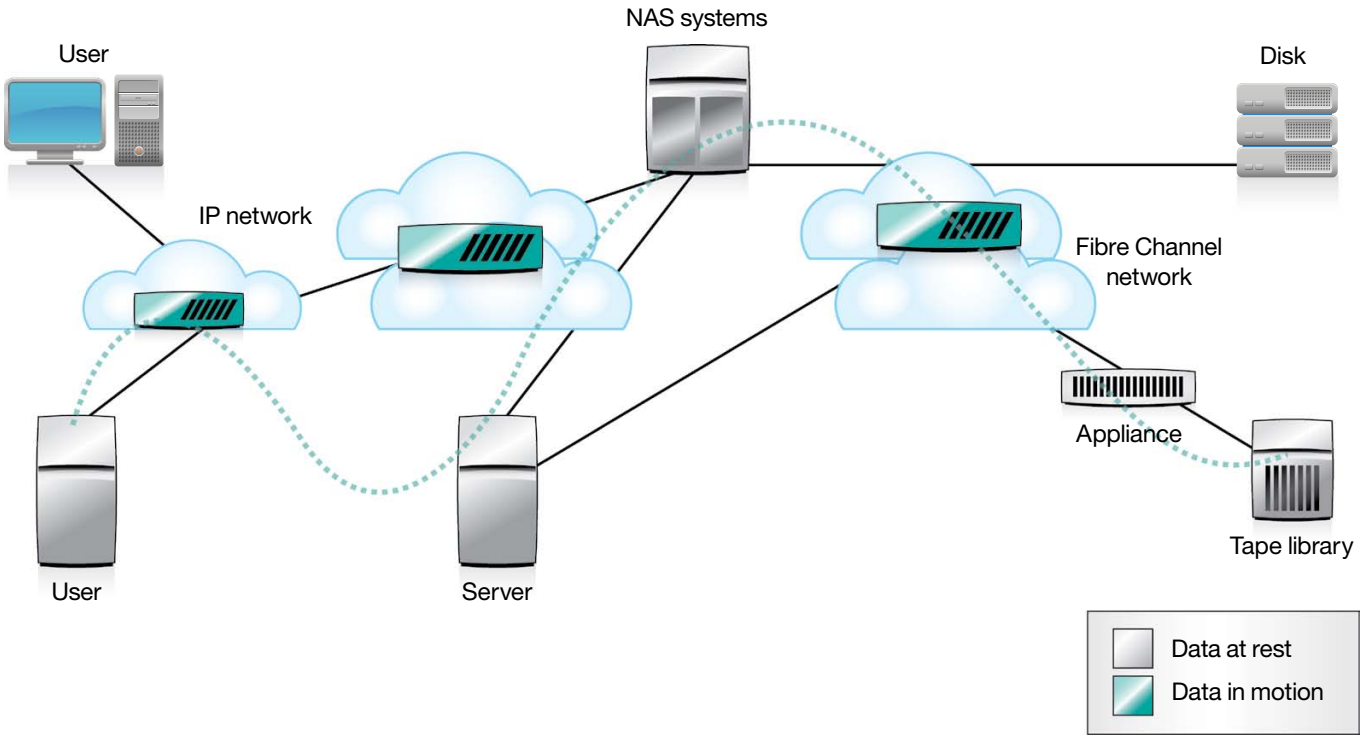
*"If a covered entity **chooses to encrypt** protected health information, and subsequently discovers a breach of that encrypted information, the covered entity **will not be required to provide breach notification** because the information is not considered 'unsecured protected health information' as it has been rendered unusable, unreadable or indecipherable to unauthorized individuals."*

—Excerpt from the HITECH Act

Typically, encryption changes the rules on disclosure of breach notifications. And although regulations might only address the encryption of financial data and personally identifiable information, other types of data, such as email addresses, can also be vulnerable for attack—and can damage an organization's reputation if the data is lost or stolen. The risks of noncompliance can also include significant financial penalties. The costs associated with security breaches are making enterprise-wide encryption look better and better, especially since selective encryption can leave data exposed that can put organizations at risk.

Deployment strategies

But what is involved in an enterprise-wide approach to encryption? Over time, organizations have used different methods of encryption to protect their data. At first, encryption mostly occurred at the network layer to protect data in motion. Organizations used techniques such as Secure Sockets Layer (SSL), Transport Layer Security (TLS) and virtual private networks (VPNs) to secure the data pipeline. Then there was the need to protect data in use, enforcing who could use it and in what way. Finally, the increasing sophistication of attackers, combined with the explosion of data stored for business insights, has motivated organizations to encrypt all data at rest—that is, data that is stored on a device or in a database.



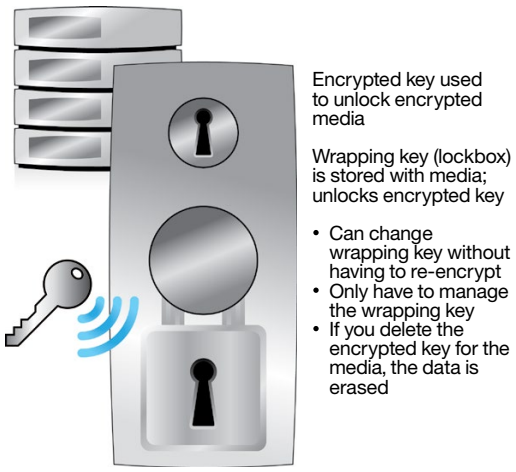
As encryption is deployed across the IT environment, there is a greater need to consolidate key management.

Use of encryption keys

Just as encryption has changed, the use of encryption keys has evolved since the introduction of the Data Encryption Standard (DES) by IBM in the mid-1970s. The simple use of symmetric keys for encryption—with the need for secret key distribution—was enhanced with the development of asymmetric keys used for authentication and techniques for the secret exchange of keys.

With "key-wrapping" or "key-encrypting" keys—built into the Trusted Computing Group (TCG) storage specifications and many IBM storage solutions—the management of keys became more practical. Now organizations need to manage only the master wrapping keys—not the individual encryption keys. The use of multiple key-wrapping keys enables functions such as secure data sharing, cloud data sanitization and cryptographic erasure (as described in NIST Special Publication 800-88).

Wrapping keys: the lockbox approach



Master "wrapping keys" eliminate the need for organizations to manage hundreds of thousands of individual keys for encrypted devices. The concept is similar to using a lockbox to access houses for sale. This strategy also aligns enterprises with supporting cryptographic-erasure, whereby the data encrypted by a key is effectively erased when the wrapping key (of the data encryption key) is destroyed.

In addition, the use of multiple keys and different types of keys is making encryption more useful for organizations by reducing the total number of keys being actively managed, simplifying administrative operations, and isolating where keys are available and under what circumstances they can be used.

The need for key management

As organizations have adopted different encryption methods—for protecting data in use, at rest and in motion—the number of encryption keys has skyrocketed. Traditionally, the more encryption you deploy, the more keys you have to manage. These keys have their own lifecycles separate from the data they're protecting—and these lifecycles have to be managed, from initialization and activation through expiration and destruction. (And this remains true, even if you need to manage only a small number of wrapping keys.)

Sometimes departmental teams manage encryption keys using manual processes or embedded tools. But in many cases, organizations have no formal, scalable approach for managing encryption keys across several terabytes of data. And this lack of an encryption key management strategy can leave the door open for loss or breaches of sensitive data.

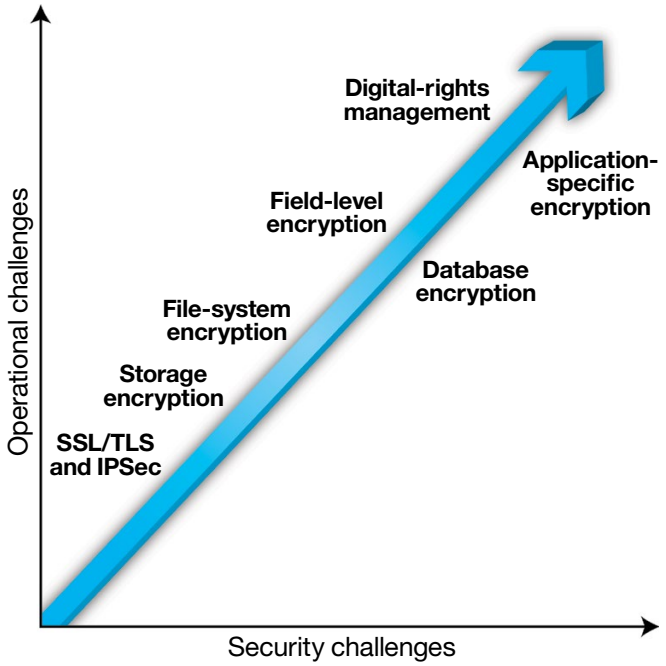
Why is it so important to manage the lifecycle of encryption keys? Some considerations include:

- Controlling your encryption keys means controlling your data. If you lose your keys, you lose your data. This makes robust key management an essential part of using encryption.
- If you lose control of the encrypted device and encrypted data, your data is still secure as long as you control the keys. It is not accessible by unauthorized users. Keeping your encryption or wrapping keys separate from your encrypting device and encrypted data assures that unauthorized users cannot recover the data without acquiring all of the pieces.

- To erase data or sanitize an encrypted device for end of life, simply power it off, and allow the device to be removed from the premises. If the key manager is unreachable from the device at its new location, the data is safe.
- Since you need the right key to access encrypted data, you can enforce access control policies by how you distribute the keys instead of attempting to manage the access to terabytes of data.

The latest key lifecycle management solutions include role-based access control, allowing you to define multiple administrators with different roles. This helps increase the security of sensitive key management operations and enables better separation of duties. In addition, different devices can be grouped into logical partitions and assigned to different administrators with different encryption keys. This enables multi-tenancy or multilayer security of a shared infrastructure—such as a public cloud—using encryption as a method for enforcing access control for each tenant.

By using strong authentication methods and temporary session keys, the latest key lifecycle management solutions can dramatically increase data security while simplifying key management. Users do not need to know anything about encryption in order to utilize the technology and realize the benefits. The data encryption is transparent to the applications that provide access to the information and to users. And performance is not impacted because each storage device has built-in technology that performs at wire speed without latency. Since organizations do not have to change their processes, install more hardware or reconfigure software to support the hardware, data security is simple and straightforward.



As organizations increase their levels of encryption, operational and security challenges also increase. The right encryption key management solution can provide the highest levels of security with the fewest operational challenges.

Centralized control of keys for any encrypting solution

Until recently, different vendors had their own key management systems with their own proprietary protocols. For example, certain encrypted drives would work only with specific key management systems. With the introduction of KMIP, the industry has a single protocol for supporting enterprise-wide encryption—removing the barriers of vendor-specific technology. Industry-standard encryption key management improves data security and provides a safe harbor to prevent the accidental disclosure or loss of information.

Centralized, industry-standard key management can help organizations:

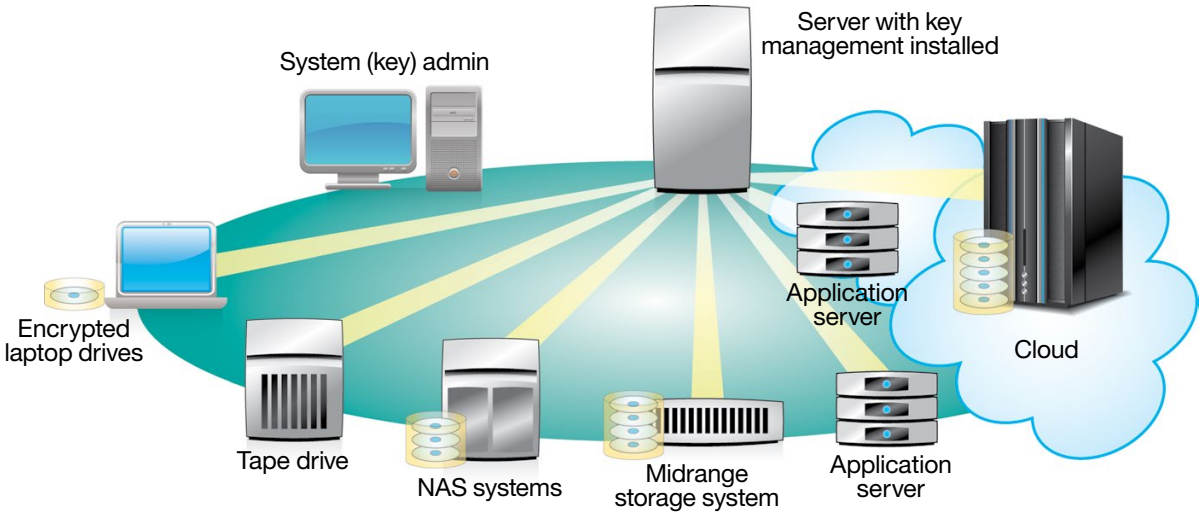
- Reduce costs related to the setup, use and maintenance of encryption keys
- Facilitate compliance with disclosure laws and regulations
- Enforce security policies and reduce risks
- Simplify the repurposing of disk drives and entire systems
- Maintain continuous, reliable access to information
- Secure backup and recovery information
- Deliver secure cloud, mobile and big-data implementations

Encryption everywhere

Many organizations today are adopting a policy of encrypting all data at rest, in addition to data in motion. One reason is that hardware-assisted encryption has removed almost all of the performance roadblocks. However, relying on encryption at the device level can still add complexity to the storage environment. As a result, organizations need an integrated, transparent way to implement encryption everywhere.

Working with self-encrypting storage and software application offerings, encryption key management solutions enable organizations to protect data when databases, disk drives or tape cartridges are physically removed from a storage system, when they are transported in-house or offsite, or even when the application or storage system is powered down. Lost storage media is not uncommon and brings with it enormous direct and indirect costs for those who lose sensitive information. But with encryption and key management solutions, organizations no longer have to worry about losing sensitive information if storage media goes for repair, becomes misplaced or is stolen. Data is unreadable until the device can re-authenticate with the key management server.

In addition, support for the KMIP standard allows industry-standard solutions to efficiently manage encryption keys across an entire enterprise environment, including self-encrypting drives, tape libraries, network-attached storage (NAS) systems, storage area network (SAN) systems, applications and storage clouds.



Using industry-standard key management solutions, organizations can automate encryption key management across their entire storage environment. The KMIP standard enables a wide range of systems to interact seamlessly.

Using encryption key management solutions, organizations can securely erase data in a matter of seconds by changing the encryption key assigned to any drive—without the help of a third-party vendor. Changing the encryption key erases the previous encryption key, and the data becomes unreadable. This protects against a data breach should a drive fall into the wrong hands. It can also minimize costs associated with securely erasing all system information when an equipment lease expires.

Meanwhile, many organizations use compression and deduplication to increase storage efficiency—but these techniques cannot be used with data that has already been encrypted by the application or by an external appliance. Encrypting within disk drives makes sense for these organizations because the encryption occurs after the compression and deduplication activities take place.

As mentioned earlier, the use of master wrapping keys helps simplify encryption key management by reducing the total number of keys an organization has to manage. In addition, with encryption built into disk drives—rather than implemented in other components—the key never leaves the drive, reducing the exposure to vulnerabilities. And since the key never leaves the drive and is unique per disk drive, the need to re-encrypt data to meet re-key requirements is greatly reduced. Organizations can re-key or refresh the authentication key used to unlock the drive on a periodic basis with no need to copy and re-encrypt the data.

Good encryption key management solutions transparently detect encryption-capable media and assign the authorization keys necessary to lock and unlock individual drives. They simplify implementation by running on most existing server platforms, leveraging the resident server's security features and using the same high-availability and disaster-recovery configurations.

Deploying encryption key management

When evaluating encryption key management options, consider whether the solutions will give you the flexibility to:

- **Manage keys within separate, but organized, silos. The right encryption key management solution can simplify complex key distribution and management, reducing administrative burdens within each silo.**
- **Have centralized control and policy-driven key management. Your encryption key management solution should allow consolidated management of keys across domains, support standards that extend management across products from multiple vendors, and integrate well into existing security-team methodologies.**
- **Count on high availability and support for disaster recovery. The leading encryption key management solutions work with a wide variety of clustering, replication and failover implementations, leveraging your current investments. To reduce the chance of data loss, look for a solution that has built-in, automatic cloning capabilities.**
- **Facilitate compliance management. Enterprises need to remain compliant with the changing regulatory world. Centralizing key management supports audits against information security practices. In addition, it also allows enterprises to properly dispose of data in accordance with their data retention policies and aligns with federal guidance on cryptographic erasure through the proper destruction of encryption keys (NIST Special Publication 800-88).**

The growing support for KMIP

Developed through a collaboration of more than 30 vendors and end-user organizations, KMIP defines a single, comprehensive protocol for communication between encryption key management systems and a broad range of enterprise applications,

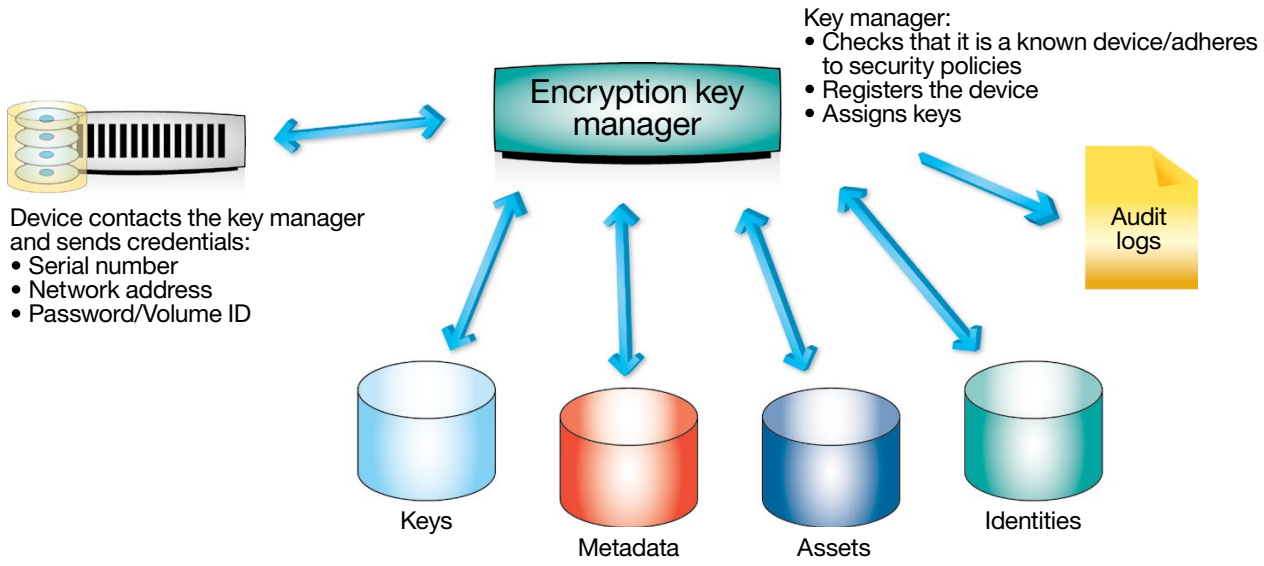
including email, databases and storage devices. This interoperability means that encryption can be used with confidence on all types of devices, from mainframes and network switches, to sensors and industry-specific devices, such as bank ATMs and smart meters.

Key lifecycle management—including the generation, submission, retrieval and deletion of cryptographic keys—is enabled by the KMIP standard, published by the Organization for the Advancement of Structured Information Standards (OASIS). Designed for use by both legacy applications and next-generation solutions such as cloud storage, KMIP supports many kinds of encryption objects, including symmetric keys, asymmetric keys, digital certificates and authentication tokens.

Given KMIP-compatible tools, organizations can manage their encryption keys from a single point of control—improving security, reducing complexity and achieving regulatory compliance quickly and easily. By eliminating the need to use redundant, incompatible key management processes, KMIP can help organizations improve data protection while also reducing the cost of maintaining multiple products.

In addition to IBM, some of the key companies participating on the OASIS KMIP technical committee include Cisco, EMC, Hewlett-Packard, Oracle, Red Hat and many others. As KMIP is integrated into their relevant solutions, the prospects for integrated key management across the enterprise are more attractive than ever.

Device credentials and the KMIP standard



IBM played an active role in helping evolve the KMIP standard to include device credentials, which helps ensure that key managers only serve keys to known devices.

What's more, the Storage Networking Industry Association (SNIA) hosts the Storage Security Industry Forum (SSIF) KMIP test program to help ensure the interoperability of KMIP-enabled products. This gives users another reason to trust in plug-and-play storage solutions.

The IBM approach to encryption and key management

Launched as the industry's first KMIP-enabled solution, IBM® Security Key Lifecycle Manager empowers organizations to take an integrated approach to encryption key management. The solution can manage encryption keys not only for IBM storage devices, but also for standards-based devices from other vendors—including Emulex, Network Appliance and Thales. Plus, it provides quick time to value with an intuitive interface and lightweight architecture.

IBM Security Key Lifecycle Manager is designed to help your organization:

- Centralize and automate the encryption key management process
- Enhance data security while dramatically reducing operations complexity
- Simplify encryption key management with intuitive features for initial configuration and ongoing management
- Help minimize the risk of loss or breach of sensitive information by making it simple to encrypt all data at rest
- Provide deployment flexibility by supporting a wide variety of operating systems and hardware devices for secure key storage
- Help facilitate compliance management of regulatory standards, such as SOX and HIPAA
- Extend key management capabilities to both IBM and non-IBM products
- Leverage open standards, such as KMIP, to help enable flexibility and facilitate vendor interoperability

Together with IBM Security Key Lifecycle Manager, IBM offers self-encrypting storage devices that support high-performance encryption without sacrificing storage efficiency. Built-in, transparent encryption enables these devices to be automatically detected by key managers, securely registered and assigned keys, and monitored for compliance—all with minimal operator intervention. Administrators need no special knowledge about cryptography, and default settings based upon the device type make configuration simple and straightforward. Different storage groups can be managed by different administrators, and the highest access levels can be limited to a few individuals on a need-to-know basis. This separation of duties aligns with security best practices and helps facilitate compliance with regulations.

In addition, IBM has played a key role in helping evolve the KMIP standard to improve security and vendor interoperability. For example, thanks to IBM involvement, the KMIP standard outlines the type of device credentials that should be provided to key managers before keys are issued, such as the device serial number, network address, instance or volume identifier, group, and shared secret. This helps facilitate compliance, since keys are only served to known devices, and also simplifies deployment, since organizations can use credentials as a right to connect rather than managing an individual certificate for each device.

IBM Security Key Lifecycle Manager helps improve security in highly regulated industries

- Blue Cross Blue Shield of Tennessee uses IBM Security Key Lifecycle Manager to simplify the end-to-end management of data protection, minimizing the time and effort needed to automatically encrypt patient data—and ensure compliance.
- The human resources department at IBM relies on IBM Security Key Lifecycle Manager to centrally manage the encryption key lifecycle for ultra-sensitive data, simplifying operations with wizard-based screens and meeting the latest audit requirements.
- Commerzbank AG in Frankfurt, Germany leverages IBM Security Key Lifecycle Manager to provide the highest level of data protection available for tape media, improving the availability of financial data for customers, investors and government regulators.

Conclusion

IBM has designed IBM Security Key Lifecycle Manager to help organizations implement a successful "encryption everywhere" strategy, leveraging standards-based key management to improve data security without sacrificing performance. Built on open standards, including KMIP, the solution delivers implementation flexibility and facilitates vendor interoperability. The IBM approach to encryption can also help dramatically reduce the number of keys administrators have to manage. By enabling centralized management of strong encryption keys throughout the key lifecycle, IBM Security Key Lifecycle Manager can help minimize the risk of exposure and reduce operational costs for the extended enterprise.

For more information

To learn more about IBM Security Key Lifecycle Manager, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/software/products/en/key-lifecycle-manager

About IBM Security solutions

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 15 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

Additionally, IBM Global Financing can help you acquire the software capabilities that your business needs in the most cost-effective and strategic way possible. For credit-qualified clients we can customize a financing solution to suit your business and development requirements, enable effective cash management, and improve your total cost of ownership. Fund your critical IT investment and propel your business forward with IBM Global Financing. For more information, visit: **ibm.com**/financing

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
August 2015

WGW03032-USEN-01