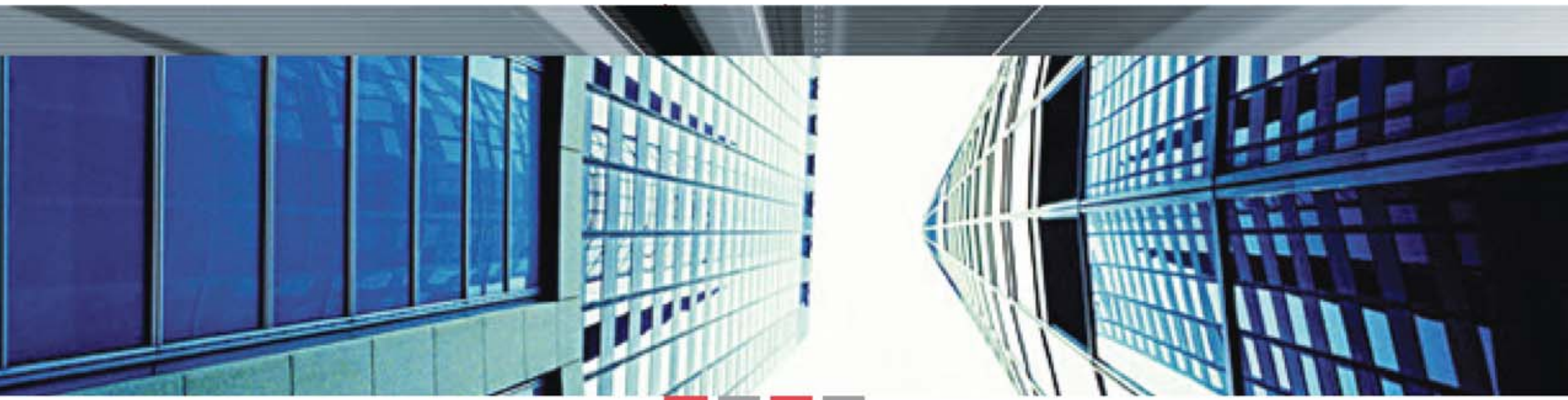

Assurency Keystone

Storage Key Management

kasten chase

SECURE INFORMATION MANAGEMENT

Assurency Keystone

Storage Key Management

2005/12/01

Kasten Chase
5100 Orbitor Drive
Mississauga, Ontario L4W 4Z4
905.238.6900
www.kastenchase.com

Table of Contents

1. Executive Summary

In the aftermath of high profile security breaches at Bank of America, Citigroup, Time-Warner and elsewhere, organizations are considering tape backup encryption with increased urgency. Many are hesitant to deploy such solutions however, fearing performance degradation, unrecoverable data through loss of encryption keys, and substantial disruptions to critical data management processes, including data protection, records retention and information sharing.

These fears are understandable and, fortunately, have been addressed. Key management systems designed specifically for data storage encryption can alleviate the concerns of the most consciencous data center manager.

These key management systems recognize that storage keys – the symmetric encryption keys used to encrypt tape backups and other storage media – are different from other types of encryption keys. Since encrypted tape backups may be maintained well into the future, storage keys must provide stronger safeguards, remain secure over their useful life, and be readily accessible in the event of data restoration at some future date. Storage key management describes the system and supporting processes that ensure storage keys are strongly protected, available when required, and non-intrusive to data protection, archiving and information sharing applications.

The attributes of a comprehensive storage key management solution include:

- Transparency to enable data management processes continue to operate unabated;
- Consolidation under a common, automated policy manager;
- High availability and scalability;
- Interoperability with enterprise key management schemas; and,
- Extensibility to a variety of encrypting storage devices.

These attributes are best achieved through adherence to open standards such as those offered by the National Institute of Standards and Technology (NIST) and the Institute of Electrical and Electronics Engineers (IEEE).

* * *

Information security and compliance are driving requirements for tape backup encryption. In time, encryption will become a ubiquitous commodity within the data storage infrastructure, and perhaps for the enterprise at large. Under this scenario, we anticipate a key management problem on the horizon – organizations attempting to manage multiple, disparate key management systems will soon be frustrated by their administrative overhead and inability to scale. To avoid these frustrations, organizations must give careful consideration to storage key management when implementing tape backup encryption. This white paper outlines these considerations and describes the attributes of Assurency® Keystone, Kasten Chase's comprehensive, storage key management platform based on open standards.

2. New Taxonomy

Tape backup encryption is a relatively new application that extends the lexicon of the storage practitioners. Some of this new terminology is defined in this section.

Cryptographic Agent

Cryptographic agent is a generic term that refers to hardware or software providing cryptographic services (e.g. encryption, decryption, key agreement, hashing, digital signatures) within a storage device such as a tape drive.

Storage Keys

Storage keys are randomly-generated, symmetric encryption keys used to encrypt data at rest on storage media.

Storage keys differ from *session encryption keys* used to encrypt data in transit. Typically, session keys are required only for the duration of an individual communications session. A new session key is created for each new communications session to enhance overall security.

In contrast, storage keys must be retained for as long as the data they protect is required. In the case of backup data, this may be a considerable period of time. The enduring quality of storage keys requires that they are cryptographically stronger (i.e. longer), well protected for possibly many years, and readily accessible to facilitate restoration from backup if required in the future.

Storage Key Management

Storage key management describes a collection of operations performed on storage keys over their useful life, including creation, distribution, retention, transfer, backup and destruction. Storage key management ensures that storage keys are well secured and can *always* be matched to the storage media they protect.

Storage key management differs from enterprise key management offered by Public Key Infrastructure (PKI) systems. As its name suggests, PKI provides policies and procedures for the issuance and management of public keys within a *public key encryption system*. An enabler for Internet e-commerce, PKI provides an effective scheme for secure transactions and information exchange between individuals unknown to each other. PKI facilitates a number of safeguards with public key cryptography, including:

- Authentication of the parties to a transaction;
- Confidentiality of information exchanged between the parties;
- Assurance that a transaction will not be altered without notification to the parties; and,
- Non-repudiation of participation in a transaction by the parties after the fact.

While PKI extends conceptually and practically to storage devices (i.e. not just individuals), it does not provide the right tools to support the long term encryption of data at rest. A comprehensive storage key management system not only provides these tools, it interoperates with an enterprise-wide PKI if and when required.

3. Data Management Processes

There is a common concern that tape backup encryption will adversely affect critical data management processes. While it is true that encryption will introduce minor latency into storage network operations, effective storage key management ensures that normal course data management processes can continue unabated. It this section, we describe three such processes, and examine the implications for both storage encryption and storage key management.

3.1. Data Protection

Since 9/11, there has been increased emphasis on ensuring business continuity in the event of disaster. For the data center manager, this means greater diligence in making backup copies of valuable data assets, protecting backup copies at offsite locations and ensuring that, in a disaster scenario, data can be restored from backup quickly and accurately.

Digital storage demand is predicted to grow at an annual rate of 30 to 40% from 2005 through 2008[1]. As a result, enterprise organizations are managing – and backing up – larger data stores. While backup windows may or may not be shrinking, there is certainly a requirement to backup more data in whatever window is available. At the same time, data center managers are pressed to improve backup processes. Recovery Time Objectives (RTOs) are decreasing while Recovery Point Objectives (RPOs) are becoming shorter, approaching almost real time data backup.

Clearly tape backup encryption solutions must not extend tight backup windows or RTOs. To ensure these objectives are met, such systems cannot appreciably degrade storage network throughput and must compress backup data before encrypting it.

In a recovery scenario, storage key management systems must ensure that storage keys are consistently and accurately paired with the removable media they protect. This matching must be infallible over the useful life of the encrypted media.

3.2. Records Retention

In the wake of financial scandals at Enron, WorldCom and elsewhere, the relevant U.S. criminal statutes and SEC rules were amended to require firms to preserve all paperwork and electronic records that might be relevant to an audit. A document retention policy provides for the systematic review, retention and destruction of documents received or created in the course of business. A document retention policy will identify documents that need to be maintained and contain guidelines for how long certain documents should be kept, reviewed for discovery, and how they should be destroyed.

Many organizations have established policies and best practices to encrypt information that is being retained for extended periods. When files are reviewed for discovery purposes, storage keys must be made available automatically and instantaneously, even for information that has been archived for 25 years or more.

[1] Storage New Horizons, Horison Information Strategies, Page 63

3.3. Information Sharing with Business Partners

Many organizations, and particularly those within the financial services sector, share customers' financial records (e.g. credit information, billing statements) with business partners as a normal course of operations. This information is routinely stored on tape and delivered via commercial means. These storage tapes are vulnerable to compromise as evidenced by the recent losses at Citigroup and Bank of America. Encryption policies and best practices are being implemented, requiring encryption of information that is shared with business partners.

Clearly, these business partners need to decrypt the storage tapes they receive. They require the storage keys – and only those storage keys – necessary to do that. The storage key management system must provide a selective and secure key transfer capability from issuing to receiving party. The receiving party may or may not have the same backup infrastructure as the issuing party. Platform-independent tape decryptors can address any incompatibilities in backup systems.

4. Enterprise Class Storage Key Management

This section outlines some of the requirements of enterprise-class storage key management.

Trusted Key Management Platform

Above all else, a storage key management platform must be trusted. It must ensure data assets are sufficiently protected well into the future. Furthermore, it must be 'locked down' – a breach of the platform exposes storage keys which in turn compromises volumes of sensitive data.

There are a number of characteristics to look for when evaluating the trustworthiness of a storage key management platform:

- Use of NIST-approved cryptographic algorithms with sufficiently long storage keys;
- Means to securely backup storage keys;
- Role-based management with multi-factor authentication;
- Physically-secure, hardened platform;
- Limited network access;
- Secure audit logs; and,
- Security certifications such as FIPS.

High Availability

An enterprise-class storage key management platform must offer redundant clustering and key replication to ensure high availability.

Centralized, Universal Storage Key Management

Over time, storage encryption will be a ubiquitous commodity, available as a standard offering in wide variety of storage devices. However, if each instance of product-based encryption includes a key management system, organizations will have to allocate additional time and resources, and will soon experience problems with scale and interoperability. Additionally, in the event of a disaster, each key management system would have to be restored upfront to gain access to encrypted data, introducing a new layer of complexity to disaster recovery planning.

For maximum leverage and flexibility, storage key management should be centralized and separate from distributed data encryption. There are a number of advantages to a centralized, universal approach.

Extensibility and Ease of Administration

A centralized, universal storage key management system can readily extend to a variety encrypting storage devices from different vendors. With such a system, organizations do not have to administrate a new management system for each new secure storage application they deploy. Multi-vendor support is best achieved with a dedicated, key management platform and a standards-based set of Application Programming Interfaces (APIs).

Centralized key management further eases the administrative burden as all storage key operations (e.g. creation, distribution, backup and transfer) can be done in one location for the entire storage infrastructure. (In addition, storage key management should be automated to the greatest extent possible and feature a highly-intuitive user interface / dashboard.)

Storage key management cannot be complex. (Complex security is underutilized security and underutilized security is clearly weak security.) It should not require that storage administrators become security experts.

Better Security

Keeping the long term repository of storage encryption keys in the same place as the encryption function is not wise from a security perspective, as the combination represents a single, lucrative point of attack. Storage keys should be available at the point of data encryption only when needed and automatically erased when any unexpected event (e.g. a physical attack) occurs. The long term repository of keys should be strongly protected. A centralized key repository can be better controlled and protected.

Scalable – High Capacity Key Repository

Enterprise-class key management systems must scale to accommodate thousands of cryptographic agents and millions of encryption keys. A single cluster should be able to span the enterprise if needed. There should not be an artificial limit on cluster size as these limits restrict scalability and make administration more difficult.

Interoperable with Enterprise Key Management Schemas

Many organizations have invested in enterprise key management schemas and PKI solutions. To leverage this investment, an enterprise-class storage key management system should integrate seamlessly with these systems.

Strong Linkages to ILM Policy Management

Clearly, an enterprise system must manage storage keys throughout the information lifecycle. It should provide a simple and intuitive way for ILM polices to translate to key management policies. For example, if an ILM policy stipulates a retention period for a particular data set, it should easily map to a destruction date for the associated storage key(s). Alternatively, if a 'records hold' decree is issued, all storage key destruction should be immediately terminated.

Based on Open Standards

Centralized storage key management, providing interoperability with multi-vendor encrypting storage devices, requires adherence to open standards such as:

- NIST standards for cryptography;
- IEEE standards for data storage encryption;
- Standard communication and communication security protocols; and
- Standard APIs.

5. The Assurency Keystone Platform

The following table summarizes the attributes of Kasten Chase's Assurency Keystone storage key management platform. It illustrates how critical data management processes – data protection, records retention and information sharing – have implications for storage encryption and storage key management.

As indicated in the table, Keystone provides all of the enterprise-class features described in section 4.

Data Management Processes	Data Protection	Records Retention	Information Sharing with Business Partners
Supporting IT Operations	Backup operations Restore operations	Data archive Data discovery Audited data destruction	Cost-effective, timely data distribution
Performance Metrics	Backup Window Recovery Time Objective Recovery Point Objective	Imposed by government and industry regulations Total Cost of Ownership over retention period	Negotiated between business partners
Implications for Storage Encryption	Support for tape and disk Strong algorithms No performance degradation	Support for object-based storage Strong algorithms Data authenticity / integrity	Support for tape Platform-independent decryption (hardware and software)
Storage Key Management Functions	Storage Key Distribution Storage Key Retrieval Storage Key Retention	Storage Key Distribution Storage Key Retrieval Storage Key Retention Audited Storage Key Destruction	Storage Key Transfer Storage Key Packaging Storage Key Export Storage Key Import
Enterprise-Class Features	▪ Trusted key management platform ▪ High availability (storage key replication) ▪ Support for mainframe and open systems ▪ Centralized and universal storage key management ▪ Scalable (high capacity storage key repository) ▪ Extensible (support for a variety of cryptographic agents) ▪ Interoperable with enterprise key management systems ▪ Strong linkages to ILM policy ▪ Based on open standards		

Figure 4-1: Keystone Storage Key Management Framework

6. Conclusion

Storage key management is emerging as one of the most critical issues in enterprise storage security. Assurency Keystone, a comprehensive storage key management platform, provides the capacity, scalability and interoperability to centrally manage encryption keys over distributed storage infrastructures. Based on open standards, Keystone was designed to support interoperability with third party encryption products and leading enterprise key management solutions. Kasten Chase encourages like-minded product vendors who see the value in centralized, universal storage key management to participate in its interoperability program.

7. About Kasten Chase

Kasten Chase (TSX: KCA) delivers innovative data storage security solutions to mitigate information security risks, meet compliance obligations and reduce the cost and complexity of data storage operations. The Company's award-winning, enterprise-class, storage security solution, utilizes a distributed, scalable architecture to encrypt networked, archive and backup storage. Kasten Chase complements its award-winning technology with business services that assess information risk and audit compliance practices for enterprise storage. Kasten Chase is headquartered in Mississauga, Ontario with offices in Ottawa, Ontario and Sterling, Virginia. Kasten Chase is a certified ISO 9001:2000 company.

For further information, please visit www.kastenchase.com or call 1.800.263.1448.

8. Disclaimer

This white paper is provided for information purposes and to promote active consideration and discussion of storage key management issues. It is not an exhaustive discussion of the issues and should be considered only as a starting point for a more complete evaluation. To the best of the knowledge, information and belief of Kasten Chase, the information in this white paper is accurate, but Kasten Chase cannot be held liable for any errors or omissions, or for any decisions based on the content.

kasten chase

SECURE INFORMATION MANAGEMENT

About Kasten Chase
Kasten Chase delivers innovative data storage security solutions to mitigate information security risks, meet compliance obligations and reduce the cost and complexity of data storage operations. To complement its industry-leading storage security solutions, the Company offers business services that assess and evaluate risk management, compliance practices and storage resource management for enterprise storage systems. BS 7799 and CISSP-qualified consultants utilize a comprehensive toolset to prioritize and cost-justify information security investments that deliver business improvements and a comprehensive foundation for compliance. Kasten Chase established its IT security credentials within government and military departments through its high-assurance, remote access solutions. Certified by the U.S. National Security Agency and pre-approved by the Canadian Communications Security Establishment, the company's RASP Data Security™ portfolio protects some of the most sensitive information in the world.