

WHITE PAPER

**The Key to Successful Data Encryption**  
**A Guide to Crossroads® TapeSentry® Key Management**



## DATA SECURITY AND ENCRYPTION IN THE ENTERPRISE

In the light of highly-publicized losses of backup tapes containing sensitive information as well the need to fulfill regulatory compliance, ensure customer privacy and abide by internal controls, corporations have grown increasingly concerned about the security and integrity of sensitive data-at-rest.

When looking at solutions for protecting sensitive information in an enterprise environment, most corporations turn to data encryption. While encryption ensures data confidentiality and integrity, it is not enough. Key management, which involves managing keys used to encrypt data, is a critical component of the total data encryption solution and is required to ensure that data is fully protected.

A total data encryption solution changes the focus of data protection from how to protect large volumes of data in a networked environment to how to manage and protect the keys used to encrypt and decrypt data. Securing and managing the keys for effective encryption and decryption is the essence of the key management challenge.

After data is protected using encryption, keys must be protected and managed with the highest level of security to ensure that data will not be accessible to unauthorized personnel. Since these keys protect a corporation's most sensitive encrypted data, control of these keys means literally controlling the "keys to the kingdom."

This paper aims to answer the following question: What are the basic elements of an effective key management implementation, and how do you choose a top-notch encryption solution?

## FEATURES OF EFFECTIVE ENTERPRISE KEY MANAGEMENT

When choosing a data encryption solution, it is important to consider robust key management, in addition to encryption algorithms. If keys are not accessible, neither is the data. If keys are too accessible, the security of the encrypted data is compromised.

Several important processes comprise key management, including secure and reliable generation, storage, archive, distribution, rotation, expiration, recovery, and deletion of keys. To reliably manage keys in an enterprise situation requires a single, turn-key, appliance-based solution. Additionally, many business goals and government compliance regulations make data encryption a requirement, with key management as the most important aspect of encryption.

## THE KEY MANAGEMENT LIFE CYCLE

Encryption scrambles data to make sure unauthorized users cannot read it, and is necessary for any storage security solution. After an encryption algorithm is chosen, a key is generated to encrypt and decrypt the data. Key management allows total control and security of these keys. To maintain a secured enterprise environment, a key must be managed from generation to deletion—the two milestones that signal the beginning and end of a key's multi-phase lifecycle, which can span weeks or years.

### *Generation*

Keys are generated using hardware and/or software, using a true hardware random number generator (RNG) or pseudorandom number generator (PRNG) based on a computer algorithm. Federal Information Processing Standards 140-2 address the security of random number generation mechanisms.

### *Storage*

Keys must be stored securely for quick and easy retrieval. Compliance regulations may require organizations to keep some types of encrypted data for predetermined periods of time. Like any critical data, keys must be backed up and stored offsite to remove the risk of loss or unintentional deletion of a key.

## The Key to Successful Data Encryption

### *Distribution*

Automated enterprise key distribution in a secure network allows keys to be given to authorized users or systems to encrypt or decrypt critical data. Authentication must be established before keys are distributed over secure networks. Key authorization may be managed through the use of smartcards or other physical tokens, which indicate that the user is authorized. For manual key exchange methods, split knowledge systems are recommended. These systems split a key among multiple users so that no single user has all the components of the key. No matter how a key is distributed, it should be encrypted at least once.

### *Rotation/Expiration*

As a precautionary measure and a security best practice, keys may need to be rotated—expired and replaced with a new key. Some organizations mandate key rotation, although it may not be required for archived data unless an older key has become compromised. Following rotation, an expired key can only be used to decrypt already-encrypted data—not to encrypt new data.

### *Recovery*

Many organizations are concerned about losing keys and, therefore, important data. Recovering keys from an archive in a data-at-rest situation is critical. Archives must be able to retain keys for extended periods of time and give access to the keys whenever the organization needs them.

### *Deletion*

To avoid unauthorized access to encrypted data, all instances of a key that has been compromised must be deleted, including those stored on backup media. Generally, key deletion is followed by the creation of a new key to re-encrypt critical data. Key management systems should include automated and manual processes to ensure that all copies of a key are deleted from all devices, archives, and backups.

In addition to including these important aspects of the key lifecycle, an effective, enterprise-class key management system should provide the following:

- A secure solution that relies on the following: the encryption algorithm; the authentication process that ensures the identity of users and systems, as well as its communication tunnel; auditing and logging; and key database security. Additional aspects of a secure solution include key storage, management, sharing, and distribution for recovery and decryption.
- A flexible solution that offers easy configuration and administration capabilities, intuitive policy management, and the ability to work with third-party key management systems.
- A manageable solution that is easy to use, with an intuitive graphical user interface, simple management of the key lifecycle, and role-based access, providing users only the options for which they are authorized.
- An available solution that can replicate and share keys to restore encrypted tapes in case of a disaster. It should also include fault-tolerant features, such as clustering of the key management server to generate and distribute keys in the case of a system crash.

## **ROBUST KEY MANAGEMENT FROM CROSSROADS SYSTEMS**

TapeSentry is a low-latency, high-performance, router-based network appliance that provides front-side compression, strong encryption, and a robust key management system to satisfy regulatory requirements and protect data stored on tape in the event of unauthorized access, theft, accidental misplacement, or loss.

TapeSentry has built its key management system in partnership with a leading key management player in the market. Purpose-built to address large and distributed encryption environments, TapeSentry uses the ERUCES Tricryption® framework to provide a secure, reliable, and scalable key management system composed of three steps. First, data is encrypted using symmetric encryption keys. Second, encrypted keys are encrypted and placed

## The Key to Successful Data Encryption

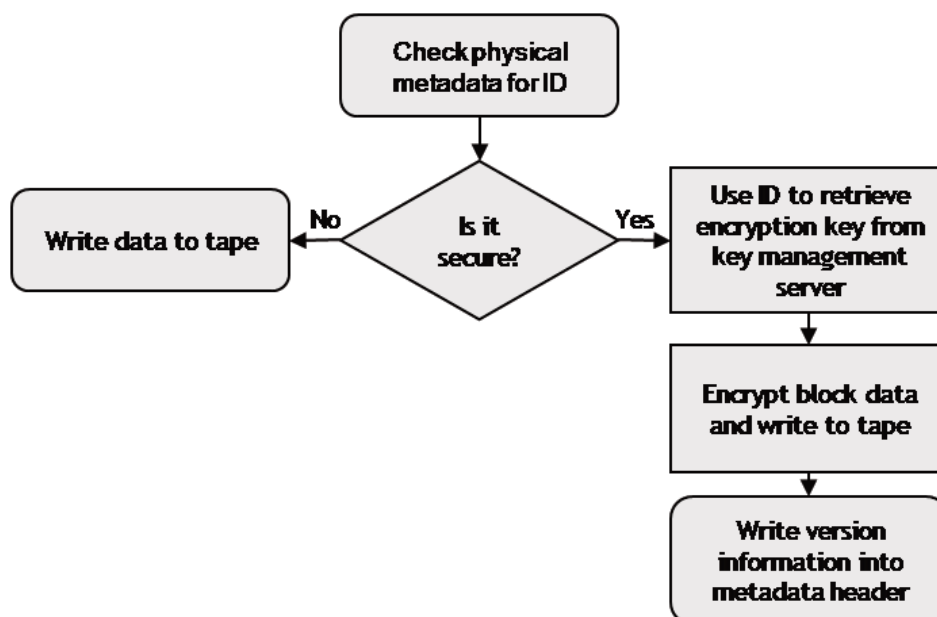
in a safe repository. Third, the link between the data and the key is encrypted and secured.

Understanding the need for a system that is both secure and flexible, TapeSentry makes keys available when and where encrypted information is read. It ensures appropriate access limitations to keys based on the requirements of the organization and the type of data being encrypted and promotes seamless integration into the enterprise security infrastructure.

TapeSentry provides unprecedented security and ease-of-use for a one-step disaster recovery solution, with secure sharing of data and keys across business partners and authorized locations.

In addition, TapeSentry can integrate with external key management systems. This flexibility allows it to coexist with other key management systems in the enterprise.

### *TapeSentry Encryption & Decryption Process*



During the encryption process, the encryption engine retrieves an ID/key pair from the key management server and stores the ID in the tape header. Each ID is associated with a unique key value assigned by the key management server, and all ID/key pairs are securely stored in the key database. The ID is used to retrieve the key from the key management server prior to decryption.

### *TapeSentry Enterprise-Class Key Management Features*

TapeSentry provides the following enterprise-class key management features:

- Key generation using a strong pseudorandom number generator
- Key storage in encrypted form in a relational database
- Key recovery that includes secure backup and restoration of the key database for complete disaster recovery
- Key sharing that occurs between multiple TapeSentry appliances with trusted relationships using mutually authenticated SSL connections

## TAPESENTRY DELIVERS ENTERPRISE-CLASS KEY MANAGEMENT

TapeSentry delivers all of the features of an enterprise-class encryption solution.

### *Security*

TapeSentry delivers maximum data security at the appliance, network, and data level. Data itself is protected by an industry-standard, robust AES-256 encryption algorithm. Role-based access and complete administrator authentication and authorization guard against unauthorized access to the box. This is coupled with Crossroads' patented access controls, a powerful resource sharing feature that controls access to storage targets from multiple hosts to the Logical Unit (LUN) level. All communication channels between the appliance and the application and between the key management client and server are secured through the use of TLS/SSL/HTTPS. The integrity of audit data is ensured through digital signatures. The device itself is secured with a custom linux kernel stripped of any unnecessary software and with no open TCP/IP ports or superuser access.

### *Flexibility*

TapeSentry leverages Crossroads' leading position of SAN interoperability in the market to provide full support for mid-range and open system servers, network infrastructures, tape devices, and libraries. TapeSentry works seamlessly with existing backup applications, and as an easy plug-and-play appliance, it effortlessly integrates into a heterogeneous tape and network environment. Market-leading routing architecture provides easy configuration of any port for host access or device connectivity as well as flexible host or target encryption policies.

### *Availability*

During a disaster, critical business data, which is often encrypted, must be restored promptly. It is vital for the decryption keys to also be available to restore this encrypted data. TapeSentry ensures the key database is backed up, and allows the automatic backup destination (NAS or SCP) to be at a secured remote site. This allows for a quick restoration of the key database at a remote site and recovery of critical business data.

### *Performance*

Operating as a fully pass-through, inline appliance, TapeSentry delivers wire-speed performance across multiple drives with minimal impact on server, network, or backup infrastructure. TapeSentry enhances data path write performance by configuring buffered tape writes and immediate data response to remove the latency created by tape devices. It provides inquiry caching that eliminates the potential for the application to respond unfavorably to slow responses from INQUIRY commands.

### *Manageability*

TapeSentry offers a superior, intuitive Web interface with a secure SSL connection and a role-based user access management system to ensure security and separation of duty between administrative and security personnel. The appliance administrator installs, configures, and administers TapeSentry; the security administrator defines encryption policies, manages certificates and users and views audit log. Additionally, TapeSentry offers complete system configuration for appliance administration, backup, and disaster recovery.

## SUMMARY

Key management is arguably the most important issue when choosing an encryption solution; the longer period of time data must be kept in encrypted form, the more important key management is to an organization. Tape Sentry addresses critical key management tenants while remaining cost-effective. Additionally, encryption appliances such as TapeSentry provide unmatched performance because of their ability to encrypt multiple data streams concurrently with no degradation in the performance of the applications spooling data to tape or of the tape drives themselves. The best encryption solution is offers robust key management and is flexible enough to integrate seamlessly with the current and future infrastructure. The result is an uncomplicated and robust tape encryption and key management appliance designed to take on your tape encryption requirements to an enterprise level.



**Crossroads Systems, Inc.**  
11000 North MoPac Expressway  
Austin, Texas 78759  
USA

**TEL:** 866.BUY.CRDS  
866.289.2737  
512.349.0300

**FAX:** 512.349.0304

**EMAIL:** sales@crossroads.com

[www.crossroads.com](http://www.crossroads.com)

**Crossroads Europe GmbH**  
Marie-Curie-Str. 19  
73529 Schwäbisch Gmünd  
Germany

**TEL:** +49 7171 99800-0  
+800 46243726

**FAX:** +49 7171 99800-10

**EMAIL:** contact-europe@crossroads.com

## ABOUT CROSSROADS

Headquartered in Austin, Texas, Crossroads Systems delivers flexible solutions to protect, secure and restore business-critical "data-at-rest." Crossroads (symbol: CRDS) is currently traded on Pink Sheets and also posts its financial disclosure reports, press releases and other related documentation on the OTCIQ web service of the Pink Sheets website. For more information, please visit [www.crossroads.com](http://www.crossroads.com).



Crossroads promotes institutional and personal environmental responsibility within the company, with our partners and with the users of our products. We are committed to providing the best products and services while encouraging practices consistent with sustainable living and resource conservation.

© 2008 Crossroads Systems, Inc. Crossroads and Crossroads Systems are registered trademarks of Crossroads Systems, Inc. Specifications may be subject to change.