DELL™
POWERVAULT™

LIBRARY-MANAGED ENCRYPTION FOR TAPE

By Libby McTeer



CONTENTS

ABSTRACT	**3**
WHAT IS ENCRYPTION?	**3**
WHY SHOULD I USE ENCRYPTION?	**3**
ENCRYPTION METHOD OVERVIEW	**4**
LTO4 ENCRYPTION BASICS	**5**
ENCRYPTION MANAGEMENT LAYERS	**5**

TABLES

TABLE 1: AME and LME Comparison	7

FIGURES

FIGURE 1: Inline Hardware Appliance Configuration	4
FIGURE 2: EKM Data Flow	8

FOR FURTHER INFORMATION AND DISCUSSION

Visit dell.com/storage

THIS WHITEPAPER IS FOR INFORMATIONAL PURPOSES ONLY, AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.

SECTION 1

ABSTRACT

Increased security for data at rest is now available via library-managed LTO4 hardware encryption on the Dell PowerVault TL2000, TL4000, and ML6000 tape automation libraries.

SECTION 2

WHAT IS ENCRYPTION?

Encryption is the process of taking clear text data and converting it to data unreadable by anyone not possessing the encrypting key. The strength of the encryption, i.e. how long it would take someone to break the encryption, is based on the algorithm used and the length of the encrypting key. Longer encryption keys provide greater security.

SECTION 3

WHY SHOULD I USE ENCRYPTION?

Due to security breaches, loss of hardware containing personal data, corporate fraud, and the growing consumer demand for the protection of personal data, the federal government has passed privacy laws. Some examples of these laws include:

- Sarbanes-Oxley for corporate financial data
- Health Insurance Portability and Accountability Act or HIPAA for personal health information within health care providers
- Gramm-Leach-Bliley or GLB for consumer personal financial data within financial institutions

These regulations require that companies disclose to the public when data is compromised. These disclosures cost companies millions of dollars in lost sales and lost reputation. LTO4 tape encryption addresses the threat model of lost or stolen tapes. If sensitive data is encrypted on the tape media, the data cannot be compromised if the tape is lost or stolen.

SECTION 4
ENCRYPTION METHOD OVERVIEW

There are 3 basic ways to encrypt data stored on tape media:

- Software encryption
- Encryption via inline hardware appliance
- Hardware encryption

Software encryption is performed by the tape backup software application prior to sending the data to the tape drive. Software encryption can be CPU intensive and can cause performance degradation on the host server depending on the type and size of the data to be encrypted. Software encryption is transparent to the tape drive/library.

When using an inline hardware appliance, the data is sent from the media server to the tape device through the appliance. The appliance encrypts the data before passing the data to the tape device. Encryption via inline appliance is transparent to the tape backup software and the tape device. This method of encryption often requires expensive third party hardware for policy and key management. Higher levels of Federal Information Processing Standards (FIPS) certification require the use of appliances for encryption to safeguard the keys used to encrypt the data. Figure 1 shows the system configuration using an inline hardware appliance.

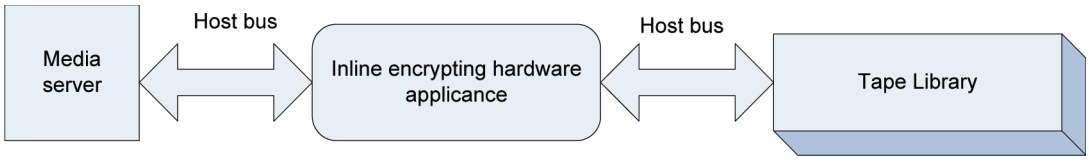


FIGURE 1: Inline Hardware Appliance Configuration

When using hardware encryption, the encryption engine on the LTO4 drive is used to encrypt the data using a key provided by the tape backup software or another external source. Hardware encryption is efficient due to the encryption function being offloaded to the drive from the CPU. Hardware encryption is also cost effective as it does not require expensive third party hardware.

SECTION 5

LTO4 ENCRYPTION BASICS

LTO4 drive based encryption was announced by the LTO consortium in January 2007. LTO4 drives use a standard Advanced Encryption Standard (AES) Galois Counter Mode (GCM) algorithm with 256-bit encrypting keys to encrypt and decrypt data on the LTO4 media. This algorithm is a National Institute of Standards and Technology (NIST) approved AES-256 block cipher. More details on the GCM algorithm can be found by searching for "Galois Counter Mode" at http://csrc.nist.gov/publications.

If compression is enabled, the drive will encrypt the data after it is compressed. The data is then reformatted to the Ultrium format before it is written to the media. Encryption can cause a 5 to 10% performance degradation due to authentication/key passing overhead and the encryption algorithm itself. Some capacity loss on the media may be experienced if small block sizes are used or if there are frequent key changes.

SECTION 6

ENCRYPTION MANAGEMENT LAYERS

On the Dell PowerVault TL2000/TL4000 and PowerVault ML6000 tape libraries, the data encryption and decryption is performed by the LTO4 full-height drives in the library. The drive alone cannot identify whether the data it receives should be encrypted or generate the encryption key. An encryption management layer is used to determine what data will be encrypted (referred to as policy) and provides the encryption key to the drive. There are two LTO4 encryption management methods:

- Application managed (AME)
- Library managed (LME)

Application-Managed Encryption

The TL2000/TL4000 and ML6000 tape libraries support application-managed encryption with a tape backup software application that supports LTO4 encryption. Currently Yosemite v8.1 SP4 and CommVault Galaxy v7.0 SP1 support application-managed encryption utilizing the LTO4 drives. Application-managed encryption support on Symantec Backup Exec 12 will be available in 2008. Please check with your Dell Technical Support Representative for the availability of this feature in Symantec Backup Exec.

In the case of application-managed encryption, the tape backup software determines what data will be encrypted and provides the key to the drive over the host bus. In addition to providing the key to the drive, the tape backup software is responsible for generating, storing, and managing the keys. Encryption is transparent to the library when using AME. AME provides greater granularity in what data is encrypted as data can be encrypted on a job basis. If application-managed encryption is selected as part of the library encryption configuration, only the tape backup software will be allowed to provide keys to the drive. A library encryption activation license key is not required for use of application-managed encryption on Dell libraries.

Library-Managed Encryption

In the case of library-managed encryption, there is very limited policy for data encryption. The only condition under which data will be encrypted is LTO4 media in an LTO4 drive in an encryption-enabled library partition. In library-managed encryption, the library serves as the proxy to provide the key to the drive from a key store in the Dell Encryption Key Manager (EKM).

How do I choose?

Security concerns should be considered when selecting between AME and LME. When AME is used, the keys are passed in the clear i.e. not encrypted between the media server and the drive over the host bus (Fibre Channel or SAS). Depending on the physical security of the datacenter, this may not be a concern for direct attach devices but the concern may be much greater in a Fibre Channel SAN environment where the connection medium is shared between multiple hosts. The T10 organization is working on a specification update to address the need to encrypt the keys prior to transmission but the tape backup software products currently only support clear key passing. Keys are never passed in the clear when using LME on the PowerVault TL2000, TL4000, and ML6000 tape libraries. Please see the next section for more information on the key passing process for LME.

AME provides finer granularity in determining what backup jobs will be encrypted. To achieve a similar level of granularity with LME, multiple library partitions would be required as well as more administration to direct backup jobs to the appropriate partition (encrypted or unencrypted).

Key management or the process of providing keys to the drive for encryption should be considered when choosing between AME and LME. AME provides centralized key management within a single tape backup software application instance i.e. Symantec Media Server, CommVault CommServe, and Yosemite Media Server. At this time, keys cannot be migrated between tape backup software instances i.e. between one CommVault CommServe instance and a different CommVault CommServe instance or between tape backup applications i.e. between CommVault and Symantec. LME provides centralized key management as the Dell Encryption Key Manager (EKM) Java application can provide keys to multiple libraries. This allows for greater interchange and migration of tapes between libraries – tapes can be interchanged between TL2000, TL4000, and ML6000 libraries as long as the libraries can access the same EKM or key store. The Dell EKM runs on Microsoft Windows 2003, RHEL 4, RHEL 5, SUSE 9, and SUSE 10, providing broad OS coverage. Maintaining the EKM does require additional responsibility for the system administrator.

Table 1 summarizes the advantages and disadvantages of application-managed and library-managed encryption.

Management Layer	Policy Granularity	Advantages	Disadvantages
Application-managed	May be more than one key per tape, may be key per data chunk or backup job	Finer policy granularity, less new responsibility for storage admin	Key passed in the clear to drive, limited centralized key management, limited interchange/migration
Library-managed	One key per tape, encryption enabled at partition level	Key encrypted when passed to drive, centralized key management – support for more OSes and applications, application agnostic	Limited policy, more responsibility for storage admin

TABLE 1: AME and LME Comparison

Library-Managed Encryption

The library-managed encryption configuration differs from a normal tape library backup configuration in that an EKM server is required to provide the encrypting keys to the drive via the library Ethernet management interface. The EKM server can be a separate server running the EKM application or the EKM server can be part of the media server. A dedicated server is not required for EKM unless system or network bandwidth limitations dictate. The only requirement is that the library has a network connection to the server and the library can reliably connect to the EKM server. EKM will work over IPv4 and IPv6 networks.

Library-managed encryption on the library is configured at the partition level. An encryption-enabled partition must contain at least one LTO4 drive. Non-LTO4 drives can reside in an encryption-enabled partition but encryption will only be supported on the LTO4 drives. All LTO4 media assigned to the encryption-enabled partition will be encrypted. Non-LTO4 media will not be encrypted even if assigned to an encryption-enabled partition. Encryption policy can be set based on internal media labels – please check your tape backup software documentation to see if it supports internal labels.

Up to two separate EKM servers can be assigned to each encryption-enabled library partition. This allows for redundancy if one server goes offline or is unavailable. The EKM servers can be configured to be identical or the servers may be different depending on the library configuration. The key stores must be the same between the EKM servers in order to allow uninterrupted access to the data on the media.

The EKM consists of a drive table, configuration file, and a key store. The drive table maintains a list of drives that has been authenticated to the EKM. The configuration file is used to configure the EKM server settings such as auto discovery of drives and key groups. The key store is an encrypted flat file containing all of the keys that have been generated for that key store. The EKM can be configured and maintained via a GUI or via a command line interface.

The key store and associated certificate can be created and populated via a GUI or via a command line interface. Keys and certificates can be added to the key store via the same methods.

The EKM also supports the use of key groups within the key store. Key groups can be used for key lifecycle management or for segregating keys by organization, company, etc. For example, key groups can be set up for each month so new keys can be used for a new month. Key lifecycle management is a manual process in EKM. The system administrator must manually reassign a different key group to the drive or drives when new keys need to be used.

The process of the EKM providing an encrypting key to the drive is outlined below and illustrated in Figure 2.

1. When an encrypted tape is mounted into the drive in an encryption-enabled partition, the drive will request an encrypting key from the EKM via the library. The library will pass the key request to the Dell Encryption Key Manager (EKM) Java application over the Ethernet management interface.
2. The EKM authenticates the requesting drive via a private key associated with the digital certificate on the drive. The drive and the EKM establish a public/private session key used to wrap the encrypting key for transit.
3. The encrypting key (DK) is fetched from the key store.
4. The encrypting key is provided to the library wrapped in the session key for security. The library provides the wrapped key to the drive via the library control port on the drive. The encrypting key is never passed in the clear between EKM and the library and the key is never stored on the media. The drive unwraps the encrypting key using the session key and uses the encrypting key to encrypt or decrypt the data as appropriate. The clear text data key identifier (DKi) provided by the EKM is written to the tape so that the encrypting key can be identified later for appends or restores. The relationship between the encrypting key and the DKi is stored in an encrypted format in the EKM.

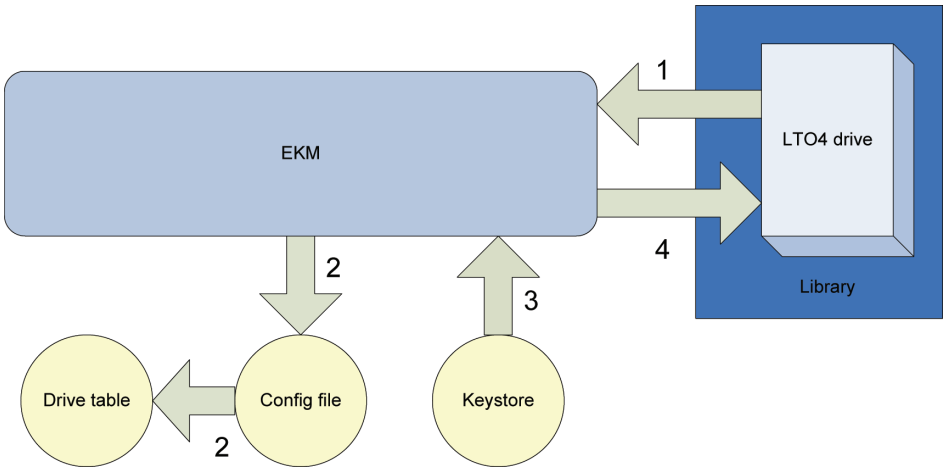


FIGURE 2: EKM Data Flow

The drive will retain the encrypting key until it is purged from the drive. The drive purges the key whenever the tape is unmounted or if power is lost to the drive. Only one encrypting key is used per tape when using library-managed encryption on the TL2000/TL4000 or ML6000 tape libraries. Depending on how many keys are in the EKM key store and how the EKM key store is configured, a key may be used for more than one tape.

Library-Managed Encryption Best Practices

Dell recommends using dual EKM servers for redundancy. If primary and secondary EKMs are configured, the library will automatically use the secondary EKM if the primary is not accessible. On the TL2000/TL4000 products, no message is provided to the user if the secondary EKM is used instead of the primary EKM. A RAS ticket indicating EKM failover has occurred is posted for the ML6000 products. Please refer to the Dell PowerVault Encryption Key Manager User's Guide for best practices for dual EKMs.

It is impossible to overstate the importance of backing up the key store once it is populated with keys and every time keys are added to the key store. If the keys are lost, the data encrypted with the keys is lost forever.

The key store should be backed up to non-encrypted media. The keys are encrypted within the key store so there is no security concern with this process. The key store should not be backed up to media encrypted with keys in the key store as the backup is no longer available if the key store is deleted or corrupted. The EKM GUI allows for the key store to be backed up every time a configuration change is made.

Test backups should be run to validate the EKM connectivity prior to starting normally scheduled backups. This will ensure that scheduled backup jobs complete successfully.

When using new media, the user must ensure that the tape backup software application recognizes the media as available for backup and is in a valid state prior to encrypting data on the media. This will ensure that scheduled backup jobs complete successfully.

When reusing previously encrypted media with a new or different key store, the following steps must be followed to erase the media to ensure that the media can be reused. Please check with your tape backup application software vendor to ensure that this functionality is supported. In CommVault under Library Properties -> Media Usage -> Overwrite Media, the two boxes (When content verification fails and When it is from different CommCell) both need to be checked in order to erase the media.

- Disable LME on the partition with the media to be reused
- Verify that LME is disabled by verifying the drive status on the library RMU
- Perform a long or short erase on the media
- Enable LME on the partition
- Verify that LME is enabled by verifying the drive status on the library RMU
- Prepare media for tape backup software use. The steps are different for each type of tape backup software. Please refer to your tape backup software documentation for this information.

To avoid data loss, periodically the EKM client or GUI should be used to validate that the EKM server or servers are still running. Once started, the EKM server should only stop if the server on which it is running is rebooted or power cycled or if the user stops the EKM server. Please refer to the Dell PowerVault Encryption Key Manager User's Guide for instructions on automatically and manually starting the EKM client and GUI and determining the status of the EKM server.

Media portability rules with LME are consistent with media portability rules between different types of tape backup software. Currently media encrypted via LME cannot be restored via a standalone drive due to lack of support for standalone drives in EKM.

To minimize the latency in providing keys to the drive, the EKM should be on a localized network. The EKM can be located on a different network or offsite from the library but the network bandwidth should be taken into account.

Libby McTeer is the tape automation lead for Dell PowerVault solutions and is the lead engineer for Dell PowerVault TL2000 and TL4000 products. She has almost 14 years of experience with NCR and Dell including server board design and ODM server design. She has a BSEE and an MSEE from Clemson University.

Exchange and SQL Server are registered trademarks of Microsoft Inc. Intel and Xeon are registered trademark of Intel Corp. Red Hat is a registered trademark of Red Hat Inc. Linux is a registered trademark of Linus Torvalds. Dell disclaims proprietary interest in the marks and names of others. ©2007 Dell Inc. A2G.