Library-Managed Encryption for Tape

Library-managed LTO hardware encryption on Dell™ PowerVault™ tape automation libraries

Dell Product Group | Storage Engineering
March 2016

A Dell White Paper

Revisions

Date	Description
January 2015	Revision 2.0
November 2015	Revision 3.0
March 2016	Revision 4.0

Acknowledgements

This paper was produced by the Storage Engineering Team.

Author: Libby McTeer – Senior Principal Storage Engineer

Table of contents

Revisions 2
Acknowledgements 2
Abstract 4
What is encryption? 4
Why should I use encryption? 4
Encryption method overview 4
LTO encryption basics 5
Encryption management layers 6
Application-managed encryption 6
Library-managed encryption 6
How do I choose? 6
Security 6
Encryption policy granularity 7
Key management 7
Dell's library-managed encryption solution 8
How to purchase IBM SKLM software 10
How to purchase library-managed encryption on the PowerVault TL1000 10

Tables

Table 1 AME and LME comparison 7

Figures

Figure 1 Inline hardware appliance configuration 5
Figure 2 Key server data flow 9

Abstract

Increased security for data at rest is available via library-managed LTO tape drive hardware encryption on the Dell PowerVault TL1000, TL2000, TL4000, and ML6000 tape automation libraries.

What is encryption?

Encryption is the process of taking clear text data and converting it to data unreadable by anyone not possessing the decrypting key. The strength of the algorithm — or 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.

Why should I use encryption?

Laws in many states require protection of personally identifiable customer data, not just notification after a security breach. Due to the proliferation of personally identifiable data like credit card numbers, businesses from self-employed service providers to large enterprise companies need to take measures to be in compliance.

Federal privacy regulations such as HIPAA covering health information and the Gramm-Leach-Bliley Act covering financial data are in the news due to data breaches. Federal privacy laws also cover the safeguard of customer data in areas such as the cable and telecommunications industry, the US census, and the department of motor vehicles.

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

Encryption method overview

There are three 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 as the data is encrypted prior to reaching the hardware.

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 (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.

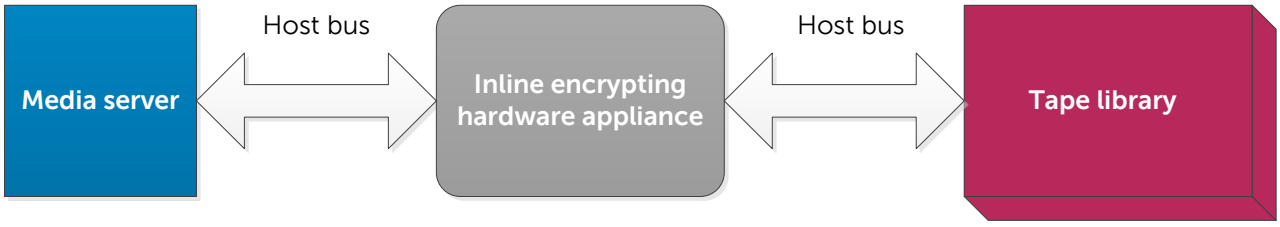

Figure 1 Inline hardware appliance configuration

When using hardware encryption, the encryption engine in the LTO-4 and later generation tape drives is used to encrypt the data using a key provided by the tape backup software or an external encryption key management server. Hardware encryption is efficient due to the encryption function being offloaded to the drive from the CPU with little or no performance impact. Hardware encryption is also cost effective as it does not require expensive third-party hardware.

LTO encryption basics

LTO drive-based encryption was announced by the LTO consortium in 2007. LTO-4 and later generation tape 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 LTO-4 and later generation media. This algorithm is a National Institute of Standards and Technology (NIST) approved AES-256 block cipher. For more details on the GCM algorithm, visit http://csrc.nist.gov/publications and search for "Galois Counter Mode".

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 slight performance degradation due to authentication/key passing overhead and the encryption algorithm itself, but should not increase the backup window. Some capacity loss on the media may be experienced if small block sizes are used or if there are frequent key changes.

Encryption management layers

On the Dell PowerVault TL1000, TL2000, TL4000, and ML6000 tape libraries, the LTO-4 and later generation tape drives encrypt and decrypt the data. 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 LTO encryption management methods:

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

Application-managed encryption

The PowerVault tape libraries support AME with a tape backup software application that supports LTO encryption. Refer to the documentation for your tape backup software to determine if LTO-based hardware encryption is supported.

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 keys 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 can provide greater granularity in what data is encrypted as data can be encrypted on a job basis if supported by the tape backup software. 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-managed encryption activation license key is not required for using application-managed encryption on Dell tape libraries.

Library-managed encryption

In the case of library-managed encryption in PowerVault tape libraries, there is very limited policy for data encryption. All data written to LTO drives in a library-managed encryption enabled partition will be encrypted. The only exception is data written to media not initially encrypted from beginning of tape (BOT). In this case, data written to media will not be encrypted.

The library serves as the proxy to provide keys to the drive from the key store in the IBM® Security Key Lifecycle Lifecycle Manager (SKLM) application. Refer to the ”

How to purchase IBM SKLM software" section for more details on obtaining the application.

How do I choose?

Security

Security concerns should be considered when selecting between AME and LME. When AME is used, the keys may be passed in the clear and not encrypted between the media server and the drive over the host bus. Depending on the physical security of the data center, 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 specification now provides a method of wrapping (encrypting) of encryption keys during transmission over the host bus. Refer to your tape backup software documentation to determine if your application supports encryption key wrapping for transmission. Keys are never passed in the clear when using LME on PowerVault tape libraries.

Encryption policy granularity

AME can provide finer granularity in determining what data will be encrypted. You can select which backup jobs to encrypt or not encrypt using the same LTO drive. 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

Consider key management — the process of providing keys to the drive for encryption — when choosing between AME and LME. AME provides centralized key management within a single tape backup software application instance, but there may be limits on encryption key migration. LME provides centralized key management as the IBM SKLM application can provide keys to multiple libraries and multiple library types such as TL1000, TL2000, TL4000 and ML6000 simultaneously. This allows for greater interchange and migration of tapes between libraries — tapes can be interchanged between PowerVault libraries as long as the libraries can access the same IBM SKLM key store. Maintaining the IBM SKLM application does require additional responsibility for the system administrator.

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

Table 1 AME and LME comparison

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 may be 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 Application agnostic	Limited policy More responsibility for storage admin

Dell's library-managed encryption solution

The library-managed encryption configuration differs from a normal tape library backup configuration in that a server running the IBM SKLM application is required to provide the encryption keys to the drive via the library Ethernet management interface. In the Dell solution, the key server is separate from the tape library. You must ensure the key server performance and response time are not affected by any other applications running on the same physical server to ensure keys are available for scheduled backups. The library and key server can communicate 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 LTO-4 or later generation tape drive. Only encryption-capable drives can be used in an encryption enabled partition; LTO-3 drives are not supported in an encryption-enabled partition. All LTO-4 and later generation media assigned to the encryption-enabled partition will be encrypted. The only exception is data written to media not initially encrypted from beginning of tape (BOT). LTO-1, LTO-2, and/or LTO-3 media will not be encrypted even if assigned to an encryption-enabled partition.

To prevent possible data loss due to a key server failure, Dell recommends using a primary and secondary IBM SKLM server setup. This configuration provides redundancy in the event that the primary key server is down or unavailable. Each encryption-enabled partition in the library can be configured for up to two key servers. The SKLM server configurations must be identical in order to allow uninterrupted access to the data on the media. The IBM Security Key Lifecycle Manager Information Center provides the documentation necessary to install and configure primary and secondary key servers. For more information, visit http://www-01.ibm.com/support/knowledgecenter/#!/SSWPVP_2.5.0/com.ibm.sklm.doc_2.5/welcome.htm (for additional languages, change the country selection at the top of the page).

The IBM SKLM application consists of a drive table, configuration file, and a key store. The drive table maintains a list of drives that have been authenticated to the key server. The configuration file is used to configure the key server settings such as auto discovery of drives. The key store is a DB2 database containing all of the keys that have been generated for that key store. The keys are obfuscated in the database and are never visible in the clear.

The following steps outline the process for providing the encryption key to the drive. See also Figure 2 for an illustrated depiction of the process.

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

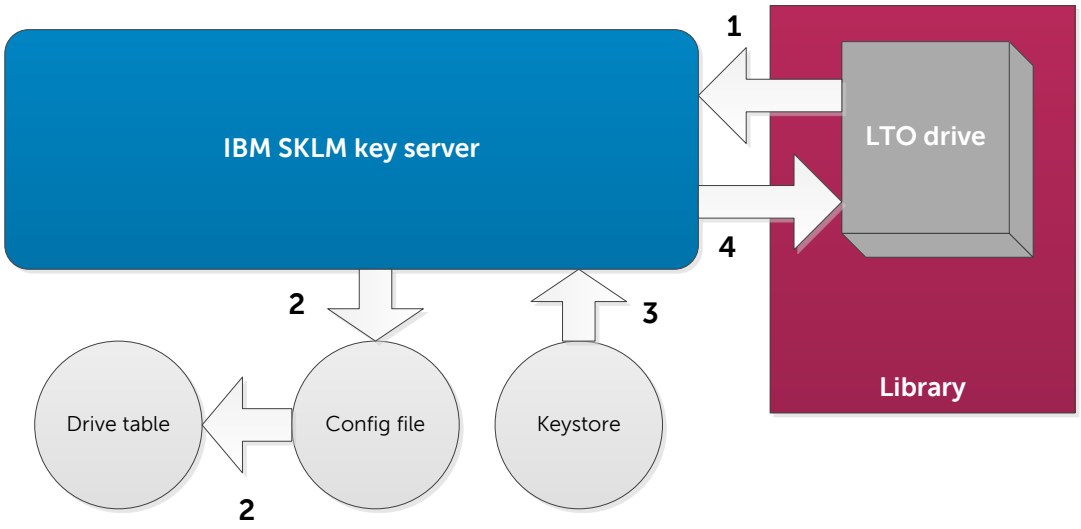

Figure 2 Key server data flow

The drive will retain the encryption key until the current media is un-mounted or until power is removed from the drive. This is to ensure the security of the encryption key when it is outside of the encrypted key store.

Only one encryption key is used per tape when using library-managed encryption on PowerVault tape libraries. Depending on how many keys are in the key store and how the key store is configured, a key may be used for more than one tape.

Please refer to the "Privacy Regulation Compliance with Dell ™ PowerVault ™ Tape Libraries" white paper for library-managed encryption reference architectures for small to medium business customers and large enterprise customers.

How to purchase IBM SKLM software

Dell customers can purchase the IBM SKLM software directly from IBM. To purchase the software within the U.S., visit http://www-03.ibm.com/software/products/en/key-lifecycle-manager-dell. To purchase software in another country, change the country selection at the top of the page. These pages only list the purchase requirements for Dell customers using PowerVault tape libraries. Dell customers with existing IBM sales relationships can leverage those relationships for purchase. SKLM drive licenses and software maintenance after the first year must also be purchased from IBM.

The sales life of the Dell Encryption Key Manager 3.0 software has ended. Customers purchasing library-managed encryption licenses for their PowerVault tape libraries will need to purchase the IBM Security Key Lifecycle Manager software from IBM.

Dell customers currently using Dell Encryption Key Manager 3.0 (EKM 3.0) can use the software through the end of support life of the PowerVault TL2000, TL4000, and ML6000 tape libraries. However, no hardware and operating system updates or fixes will be available for the EKM 3.0 software. Customers needing operating system updates such as Microsoft Windows 2012 or hardware updates such as LTO-7 and the TL1000 will need to purchase the IBM SKLM software.

How to purchase library-managed encryption on the PowerVault TL1000

Library-managed encryption enabled PowerVault TL1000 tape libraries can be purchased at point of sale only. Library-managed encryption cannot be enabled on existing TL1000 tape libraries and the feature cannot be purchased after point of sale as is the case with other PowerVault tape libraries.

Library-managed encryption is only available on LTO-6 and later generation TL1000 tape libraries. Customers currently utilizing LTO-4 encrypted media will need to purchase the LTO-6 configuration due to the n-2 backwards compatible read limitation of LTO drives and media.