# White paper
# FUJITSU Storage ETERNUS LT Data Encryption and Key Management

All ETERNUS LT systems encrypt the backup data autonomously with hardware encryption through the LTO tape drive offering enhanced security and compliance. Safeguard your backup data in the ETERNUS LT!

## Contents



## Introduction

Data Encryption provides the ability to encrypt data both for transmission over non-secure networks and for storage on media. The flexibility of key management schemes makes data encryption useful in a wide variety of configurations.

Three basic data encryption procedures exist: source, software and hardware encryption, whereby the two latter are the most suited for encryption during data backup. In contrast, source encryption is already applied with the file system (e.g. Windows Encrypting File system) or database (Oracle). The disadvantages of this method are losses in performance, increased key management costs, because each system generates its own key, and the difficulty that backup systems can no longer compress encrypted data.

As to whether software or hardware encryption is used is a question of cost and the required security level. Software encryption can be implemented more cheaply, but usually does not meet the highest security standards required by an interaction between server hardware and encryption software. And encryption via software also impairs server performance due to the greater computing requirements. Hardware appliances, which have an own processor and memory for enciphering, are expensive, but also faster, and also meet the highest security standards, such as FIPS 140-2 (Federal Information Processing Standard) – which is the US American encryption standard for the public sector.

Regardless of the solution chosen, it is important to have sophisticated key management, which automatically generates, enciphers and stores the keys and then assumes the management of the keys with the backup system. Once started, these solutions then perform their services without any additional administration expense. The LTO-4 standard represents a major step forward for the encryption of tape storage systems without any performance losses in the backup process.

The fourth generation of LTO standard of the LTO consortium, consisting of Hewlett-Packard, IBM and Quantum, which was agreed in January 2007, requires the drives to be able to encrypt the data during write by »AES 256 bit« algorithm. This encryption complies with the security standard recommended by the US Government for data classified as "top secret".

When it comes to allocation, application and control of the keys for encryption in the LTO-drive, the solutions of the manufacturers of backup hardware and backup software are differentiated by the upstream key management. However, there is one thing all manufacturers do agree on: Implementation should be on a redundant basis on two servers with the key management software and two hardware appliances in the RAID-1 array in order to ensure access to the encrypted data in case of a failure. And with all the solutions it is possible to export the keys and, if necessary, use them to set up a new system. If these options - second system and/or key export - are not used, the backup data can no longer be read if the hardware fails - not even by data recovery experts.

## Encryption standards and hardware encryption

The Federal Information Processing Standards (FIPS) are a set of standards that describe document processing, standard algorithms for the search in digitalized information and provide other standards for information processing in governmental authorities. The FIPS 140-2 standard specifies the security requirements for cryptographic modules. It describes the approved security functions for symmetric and asymmetric key encryption, message authentication, and hashing. For more information about the FIPS 140-2 standard and its validation program, see the National Institute of Standards and Technology (NIST) and the Communications Security Establishment Canada (CSEC) Cryptographic Module Validation Program website at http://csrc.nist.gov/groups/STM/cmvp.
The FIPS-compatible 256-bit AES algorithm is normally used for all encryption purposes. This also includes generating passwords in order to restrict access to the restore and import functions of encrypted data.

Only data that is not already available in an encrypted form is encrypted. Various starting points are possible to encrypt data in accordance with the security requirements of a company. The earlier the encryption runs during data backup, the more secure the data traffic is from the backup server to the medium. However, encryption has an impact on the time slot for the data backup, because it influences the performance of the backup server and/or the backup client.

The starting points for encryption during backup are:

- Encryption of the data at the backup client (or agent)
- Encryption of the data at the backup server during data backup
- Encryption of the data during migration from hard disk to tape drive (two-stage data backup or so-called "disk-to-disk-to-tape" procedure)

When data encryption is used, the time slot for the data backup increases, because the encryption requires CPU time on the backup server or backup client. The use of hardware-based encryption in the LTO tape drives of the ETERNUS LT product series permits faster encryption, as the CPU of the backup server or the backup client is relieved of this task. As independent sub networks, which are separated from the production network, are usually used for data backup in the data center, the risk for unencrypted data on these sub networks is rather low. Therefore, when using ETERNUS LT, Fujitsu recommends that the encryption is performed during backup (or during migration in case of a two-stage backup) using the hardware-based encryption procedure of the LTO tape drives in the ETERNUS LT product series. The encryption is carried out on the backup server during the write procedure to tape, and only the encrypted data is written to the medium.

## Hardware Encryption in LTO drives

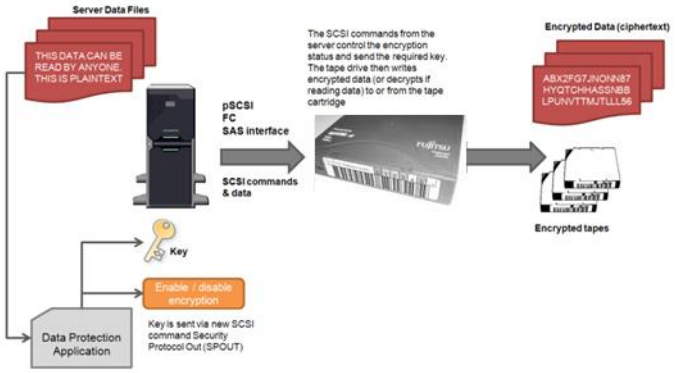
The tape storage systems of the ETERNUS LT series are based on the proven LTO technology, which combines large capacity, high speed and very low media costs. These tape storage systems can be equipped with LTO tape drives, which enable integrated data encryption during backup. The tape drives are able to independently encrypt data when it is written to tape. After the hardware-based data compression, the speed of the tape drive can almost be fully utilized. The encryption process influences the performance of the read/write speed by less than one percent. Relocating the encryption into the tape drive increases the speed of the data backup and relieves the load on the CPU of the server that carries out the backup.

Hardware encryption through LTO drives is specified as part of the LTO standard since the LTO-4 generation. For this purpose, a 256-bit AES (Advanced Encryption Standard) algorithm in Galois Counter Mode on

an encryption processor (ASIC) has been integrated into the electronics of the tape drive. This implementation supports the IEEE P1619.1 standard for the encryption of tapes and the SCSI T10 standard, which are used in numerous backup programs.

The LTO tape drives of the ETERNUS LT series use the 256-Bit AES algorithm for data encryption. This is a random bit sequence which was especially developed to encrypt and decrypt data. This algorithm has been optimized to ensure that the key it generates is unique and random. The longer the password that is used for the key, the more difficult it is for it to be deciphered by the key generated by the algorithm.

The following diagram provides an overview of the encryption process in the LTO tape drives:




The unencrypted data is sent from the backup server and runs through the SCSI interface of the tape drive. The SCSI commands sent by the backup server check the status of the encryption and the key used for the encryption. The tape drive then compresses and encrypts the data before it is written to the tape as an encrypted character string.

The fact that the hardware encryption is anchored in the LTO-4 standard ensures that LTO tape drives of LTO-4 generation and higher can decrypt the data encrypted by all manufacturers if an encrypted medium and the key used are available.

The exchange of encrypted media between the various tape drives is ensured by the standardized procedure, if the tape storage product supports the hardware encryption. The LTO-5 tape drives also read LTO-3 media and can also write to and read LTO-4 media. However, data encryption is only a supported feature for LTO-4 media or higher generations. The backwards compatibility is valid for all generations of LTO drives and media.
Keep in mind that tape media needs to be grouped and capable of encryption, too. For later decryption the tape media must be placed in a drive that is capable of decryption. Using earlier LTO versions than LTO-4 for reading and writing, the data cannot be encrypted. For example, LTO-4 drives can read LTO-2 media, but the LTO-2 media cannot be written in either unencrypted or encrypted format.

The Encryption in the tape drive is enabled by two newer SCSI commands, which are included in the SCSI T10 standard. The commands are "security protocol in" (SPIN) and "security protocol out" (SPOUT). SPOUT is used to enable encryption and in order to set the key, and SPIN is used to determine the status of the encryption.

## Key Management via Backup Software

### General overview

The 256-bit AES algorithm used for hardware encryption uses a secret, symmetric key, which is required for the encryption and decryption of data. For security reasons the key is never written to the LTO medium and the key used is only known to the tape drive until the tape drive is switched off or reset (restart, power failure, etc.). The tape drive must then either be supplied with the key again or a new key. The keys for this are sent to the tape drive by means of a SPOUT SCSI command. As a rule, a new key is sent to the tape drive for every data backup and for every tape used.

The data linked with the key is written to the tape medium in plain text (unencrypted), which is referred to as "Additional Authentication Data" (AAD) or "Authenticated Key-Associated Data" (AKAD). This data is used by a key management system as a reference to the keys that are used and saved when the encrypted medium is created in the database of the key management system. Backup software is thus able to find the correct key in the key management system if an encrypted medium has to be read in order to recover data. If an encrypted tape medium is to be read, the correct key must be taken from the key management system database by the backup software and transferred to the tape drive so that the encryption processor of the tape drive can decrypt the data.

All major backup software applications like Symantec NetBackup, Commvault software, et cetera are supporting data encryption and integrated key management. All ETERNUS LT tape libraries equipped with LTO-4 drives or higher support the key management via backup software. Key allocation and administration is performed on the tape by the backup server, where these keys are then also used for communication with the virtual LTO drives of the virtual tape library.

A backup procedure with this on-the-tape solution is as follows:
- The backup software sends a command for data backup on tape X to an LTO-tape drive of the ETERNUS LT. The tape drive requests a key from the key management of the backup server. The key management of the backup software generates a key and returns it to the drive. The drive encrypts the data with the key received, and thus establishes a relationship between the tape and the key. The link between the key and the tape is then saved as AAD or AKAD in the tape header and in the key management database. The LTO tape medium is thus encrypted.
- If the backup software requests tape X for a restore, this tape is inserted into the LTO drive. The drive requests the correct key, which it receives via the backup software from key management, and deciphers the data for restore.

Passwords, from which a key is created with the AES 256-bit algorithm, are required in order to encrypt the LTO media. These passwords are normally longer than passwords that are used by administrators or users for system logons, and they consist of several words or text groups. Good passwords for the creation of keys should be between eight and 128 characters in length. Fujitsu recommends you to use passwords for AES encryption with more than the minimum number of characters. Effective passwords include letters in both uppercase and lowercase as well as numbers and special characters. Quotes from literature and other texts should not be used as passwords.

If the backup software with integrated key management is used, either a cluster solution or well organized, regular key export should on account of the redundancy required in the introduction be provided.

**Commvault Software**

■ Data Encryption - Overview

Data Encryption provides the ability to encrypt data both for transmission over non-secure networks and for storage on media. The flexibility of key management schemes makes data encryption useful in a wide variety of configurations.
The Crypto Library module supports data encryption methods approved by the Federal Information Processing Standard (FIPS) as well as additional data encryption methods not approved by FIPS. To verify the method that the software is using, see Verifying the Data Encryption Method. The National Institute of Standards and Technology has Commvault's certification under the list of Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules that have been tested using the cryptographic module validation program (CMVP).

Data Encryption by using Commvault software can be specified at the following levels:
– Client level (for backup)
Client level encryption allows users to protect data prior to it leaving the computer. You can setup client level encryption if you need network security. The data encryption keys are randomly generated per archive file.
– Replication Set level
Encryption for replication is specified on the Replication Set level, and applies to all of its Replication Pairs. For a given Replication Set, you can enable or disable encryption between the source and destination machines. Replication Set level encryption encrypts data on the source computer, replicated across the network to the destination computer, and decrypted on the destination computer.
– Auxiliary Copy level (for copies)
Auxiliary Copy level encryption encrypts data during auxiliary copy operations enabling backup operations to run at full speed. If you are concerned that media may be misplaced, data can be encrypted before writing it to the media and keys stored in the CommServe database. In this way, recovery of the data without the CommServe is impossible - not even with Media Explorer.
Here, data encryption keys are generated per storage policy copy of the archive file. Thus, if there are multiple copies in a storage policy, the same archive files in each copy gets a different encryption key. Individual archive files, however, will have different encryption keys.
– Hardware level (all data)
Hardware Encryption allows you to encrypt media used in drives with built-in encryption capabilities, which provides considerably faster performance than data or auxiliary copy encryption. The data encryption keys are generated per chunk on the media. Each chunk will have a different encryption key.
More information about Data Encryption using Commvault Software
http://documentation.commvault.com/commvault/v10/article?p=features/data_encryption/data_encryption.htm

■ Hardware Encryption and Key Management

Hardware encryption is supported by all MediaAgents, if the devices attached to these MediaAgents support encryption. Note that hardware encryption is only supported by tape libraries. Hardware encryption is not applicable for disk library.

From LTO-4 technology onwards the tape drives support encryption of data on the tape drive. These tape drives provide the necessary controls to the backup applications to get the encryption capabilities as well as set the encryption properties on the drive. The Hardware Encryption feature of Commvault software provides key management for those tape libraries which do not support key management by themselves.

Key Management for Hardware Encryption can be enabled in one of the two ways:
1. Commvault Software managing the encryption keys
If the library does not have a license to enable the key management, then you can enable it from the Storage Policy copy level.
Key management includes the ability to generate random encryption keys for stored data and also manage the secure storage of these keys. In addition, it also includes the ability to provide a random encryption key for the tape drive to perform the encryption and decryption of the data. The random key is generated for each chunk in the media so that the strength of the encryption is very high. If all the data in a media is encrypted with the same key, it is susceptible to breakages and thus will have lower strength.
This random key is generated based on FIPS (Federal Information Processing Standard) standards and the same key is not reused for other backup data.
Hardware encryption must be established for each data path and is only available for data paths that direct data to tape libraries.
For each data protection operation, the software checks the drive to see if encryption is supported. If encryption is supported, the software provides the encryption key, which is in turn stored in the CommServe Database Engine when the chunk is written to the media. The encryption key will be stored after scrambling it with a proprietary encryption.
The encryption key gets deleted when the data for that chunk is pruned.
– Hardware encryption must be enabled only when the drives associated with the data path support encryption. If this option is enabled and the hardware does not support encryption, jobs using the data path will go 'Pending'.
– For Data Recovery and Auxiliary Copy operations using the CommCell Console, the specific key will be automatically provided by the software for each chunk.
– For Data Recovery operations using the Media Explorer, an option to store the encryption key on the media is provided in the data path.

2. Hardware or Library Managing the Encryption Keys
Some of tape libraries like ETERNUS LT260 also provide key management services.
If you have a hardware vendor license applied on the library for key management, and it is enabled, then no additional Commvault Software license and / or configuration are required. In this scenario, the encryption and key management will be done at the hardware level.

More information about hardware encryption see Commvault software OnlineBooks:
http://documentation.commvault.com/commvault/v10/article?p=features/data_encryption/hardware_encryption.htm

**Veritas NetBackup**

- Data Encryption

Verifying an encryption backup:
When NetBackup runs a tape-encrypted backup, and the administrator views the Images on Media, the administrator see the encryption key tag that is registered with the record. This key tag is the indication that the data written to tape was encrypted. The encryption key tag uniquely identifies which key was used to encrypt the data. The administrator can run a report and read down the policy column to determine whether everything on a particular tape was encrypted.

- Key Management

The NetBackup Key Management Service (KMS) feature is included as part of the NetBackup Enterprise Server and NetBackup Server software. An additional license is not required to use this functionality. KMS runs on NetBackup and is a master server-based symmetric Key Management Service. It manages symmetric cryptography keys for the tape drives which have a built-in hardware encryption capability (LTO-4 and higher) and conform to the T10 standard. KMS has been designed to use volume pool-based tape encryption. A SCSI command enables encryption on the tape drive. NetBackup accesses this capability through the volume pool name.

The configuration of KMS is done by creating the key database, key groups, and key records. Then NetBackup is configured to work with KMS. KMS generates keys from customers' passcodes or it auto-generates keys. The KMS operations are done through the KMS command line interface (CLI). The CLI options are available for use with both 'nbms' and 'nbmkmsutil'.
KMS has a minimal effect on existing NetBackup operation system management and provides a foundation for future Key Management Service enhancements.

The NetBackup KMS uses the NetBackup Cryptographic Module which is FIPS validated and can be operated in FIPS mode. For more information see: NetBackup Security and Encryption Guide, chapter 8: http://www.veritas.com/docs/000004642 ).

More information and considerations that relate to the functionality and use of KMS, see: http://www.veritas.com/docs/000075382

## Key Management via Tape Library

### General

Some tape libraries like ETERNUS LT260 provide key management services via the library.
The encryption and key management will be done at the hardware level. The hardware library generates and stores the encryption keys per media and the hardware drive encrypts the data. Therefore, every backup job written to a specific media will have the same key.

### ETERNUS LT260 supports KMIP

- KMIP Standard

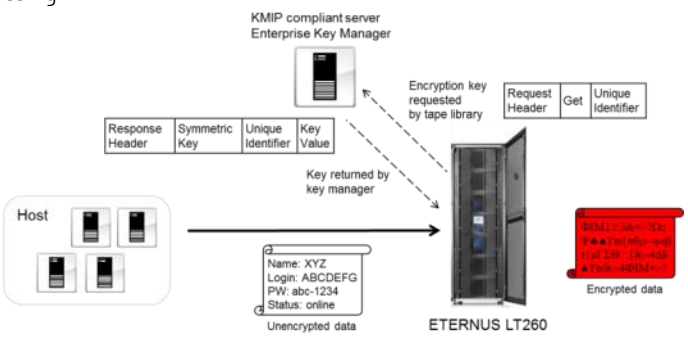
The Key Management Interoperability Protocol (KMIP®) is a specification developed by OASIS®. The first version of KMIP was formally ratified on October 2010. Its function is to standardize communication between enterprise key management systems and encryption systems.

In many IT environments there exist different key management systems within a network. The key management system for application, database or file encryption varies from encryption systems for disk or tape. Even in those cases where a single key management system can support multiple types or kinds of encryption systems, there are typically different communication protocols between the key management servers and each of the cryptographic clients.
The Key Management Interoperability Protocol (KMIP) addresses and solves these challenges. The KMIP is a standardized protocol for the communication between cryptographic clients that need to consume keys and the key management systems that create and manage those keys.
This low-level protocol enables fully interoperable key management. By using KMIP enterprises can deploy a single encryption key management infrastructure to manage keys for all applications, devices and systems.

- KMIP with ETERNUS LT260

The Fujitsu Storage ETERNUS LT260 tape system supports the Key Management Interoperability Protocol (short: KMIP) standard for exchanging encryption keys over the network. The KMIP key management software is installed on an external KMIP compliant key server.

KMIP defines a standard message format for exchanging these and other cryptographic objects between enterprise key managers and cryptographic clients. The following figure shows ETERNUS LT260 by using KMIP.




In this diagram, the ETERNUS LT260 with encrypting tape drives has received information from a host system in plaintext form and needs to encrypt that information when writing it to tape. The tape system sends a request to the key management system for a "Get" operation, passing the unique identifier for the cryptographic object, in this case a symmetric encryption key which the library needs to encrypt that particular information. The key management system returns attributes for that object, including not only the value for that key, but also other attributes, such as the kind of key (symmetric) and the unique identifier. The attributes guarantee that the storage system is receiving the correct key. Headers for both - the request and response - provide information such as the protocol version and message identifiers. The participating systems within the KMIP network use this information to track and correlate the messages.

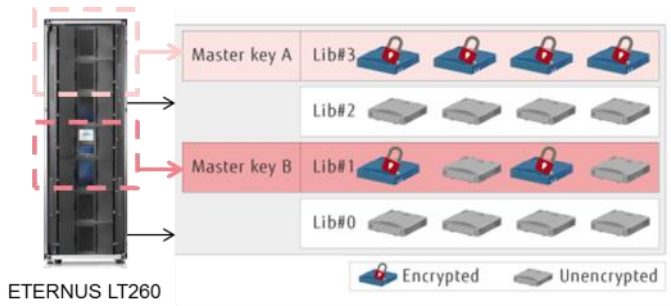
The KMIP key management functionality of the ETERNUS LT260 requires a separate license for the ETERNUS LT260.

The KMIP implementation of ETERNUS LT260 is based on the KMIP specification 1.2 and KMIP Tape profile 1.0.
For details about the specifications see:
KMIP specification 1.2:
http://docs.oasis-open.org/kmip/spec/v1.2/os/kmip-spec-v1.2-os.html
KMIP Tape profile 1.0:
http://docs.oasis-open.org/kmip/kmip-tape-lib-profile/v1.0/kmip-tape-lib-profile-v1.0.html

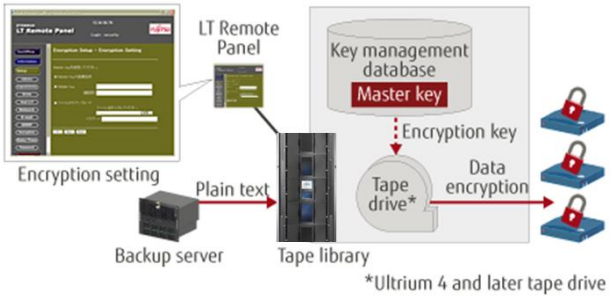
### Key Management via ETERNUS LT260

The ETERNUS LT260 generates and manages data encryption keys within the library without the expense of a backup software license or the need of an additional server for the encryption key management.
The optional Key Management Function of the ETERNUS LT260 enables easy construction of a secure backup system independently of the operating system and backup software, since the tape library will automatically handle encryption.

The Key Management Function uses two types of keys for encryption: the master key and the encryption key.
The library software generates a single and unique master key per logical ETERNUS LT260 library. (The partitioning option divides one ETERNUS LT260 in several logical libraries, see ETERNUS LT features: Partitioning).
The tape library automatically creates the encryption key and provides the key to the target tape cartridge. The encryption key is based on the master key and is assigned to each tape cartridge in the tape library. The keys are redundantly stored in a database within the library.




During data backup from a backup server, the tape library automatically assigns an encryption key to the specified data cartridge, encrypts the data (plaintext), and saves the data. The encryption process during this time is invisible to users.




To share data among multiple tape libraries, Fujitsu recommends setting the same master key as the common master key for all existing ETERNUS LT260 libraries within the same data protection environment. The operation with a common master key facilitates and simplifies the use of encrypted tape data among all these tape libraries. ETERNUS LT260 with different master keys can only read encrypted data cartridges from another ETERNUS LT260, if the encryption key had been exported in advance using the encryption key export or import function.

Encrypted/Unencrypted settings can be selected for each tape cartridge and each logical library via the central ETERNUS LT260 remote management console. The library administrator can ensure the security of the library, without the intervention of the backup operator.

The optional Key Management Function requires a separate key management license for the ETERNUS LT260.

For more details see the User Guide:
ETERNUS LT260 Key Management Function Option User's Guide

**Contact**
Fujitsu Technology Solutions GmbH
Mies-van-der-Rohe-Str. 8
80807 Munich, Germany
E-mail: storage-pm@ts.fujitsu.com
Website: www.fujitsu.com/eternus
2016-01-18 WW EN