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 by using several security encryption options!

Content

1. 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.

- Data Encryption standards

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.

- Encryption Procedures:

Three basic data encryption procedures exist: source, software and hardware encryption, whereby the two latter are the most suited for encryption during data backup:

- Source encryption:
  The file system (e.g. Windows Encrypting File system) or database (Oracle) already provides source encryption. 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.

- Software Encryption:
  Implementing software or hardware encryption depends on cost and the required security level. In general software encryption is cheaper, but usually does not meet the highest security standards required by an interaction between server hardware and encryption software. In addition, encryption via software impairs server performance due to the greater computing requirements.

- Hardware Encryption:
  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.
  Hardware encryption by using tape technology is easy since the launch of the fourth generation of Linear Tape-Open (LTO). The LTO consortium, consisting of Hewlett-Packard Enterprise, IBM and Quantum, is developing LTO tape drive technology which encrypts the data during write by »AES 256 bit« algorithm. This encryption process complies with the security standard recommended by the US Government for data classified as "top secret". This LTO standard represents a major step forward for the encryption of tape storage systems without any performance losses in the backup process.

- Keymanagement:

- 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.
- 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 differ 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. All solutions can export the keys and, if necessary, use the keys to set up a new system. If these options - second system and/or key export - are not used, the backup data is not readable if the hardware fails - not even by data recovery experts.

This white paper concentrates on describing hardware encryption with LTO tape drives and several key management options for tape storage in general and in particular for FUJITSU Storage ETERNUS LT tape family.

2. Hardware Encryption

2.1. General Overview

Hardware encryption encryptes only data which is not already available in an encrypted form. 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 disk to tape drive (two-stage data backup or so-called "disk-to-disk-to-tape")

The time slot for the data backup increases by using data encryption, 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 FUJITSU Storage ETERNUS LT tape family permits faster encryption, as the CPU of the backup server or the backup client is relieved of this task. The risk for unencrypted data on these sub networks is rather low by using independent sub networks for backup, which are separated from the production network.
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.

2.2. 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 numerous backup programs are using.
The 256-Bit AES algorithm is a random bit sequence especially developed to encrypt and decrypt data. The optimized algorithm generates a unique and random key. The longer the key password the more difficult to decipher.

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

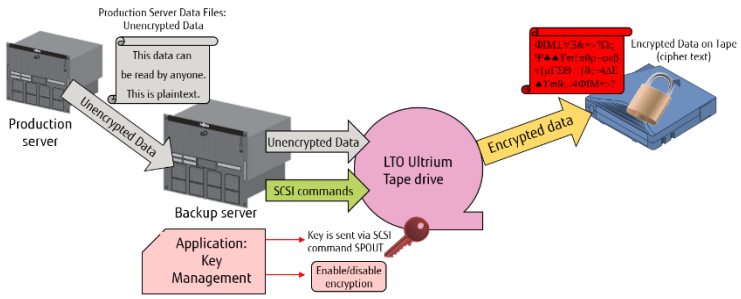


Figure 1: Tape Encryption Process

The unencrypted data is sent from the backup server and runs through the SCSI interface of the tape drive. The backup server send SCSI commands, which check the status of the encryption (SPIN) and send the key used for the encryption (SPOUT). The tape drive then compresses and encrypts the data before writing 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 implemented since the fourth generation of LTO standard. 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.

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.

3. Key Management via Backup Software

3.1. 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 Veritas NetBackup, Commvault software, et cetera are supporting data encryption and integrated key management. All ETERNUS LT tape libraries with LTO-4 drives or higher support the key management via backup software. The backup server performs the key allocation and administration on the tape, 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 media 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 media and the key. The link between the key and the tape media 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 media X for a restore, the library inserted this tape media X 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.

3.2. Commvault Software

3.2.1 Software Encryption

Software encryption encrypts the data during a backup job, a data replication job, and an auxiliary copy job (encrypts the backup data while copying the data to secondary copies).

The software encryption uses symmetric cryptography where the same key is used for encryption and decryption. So, there is no need for a certificate or a certificate authority.
In addition, the software does not encrypt a data set with a single key. Instead, the software generates a key for every stream (archive file) of data that is written which means that there is an extremely minimal chance of the entire data being lost even if the key is compromised.

The Crypto Library module supports the software encryption methods approved by the Federal Information Processing Standard (FIPS) as well as additional software encryption methods not approved by FIPS. The National Institute of Standards and Technology (NIST) has the Commvault's FIPS 140-2 Certified Crypto Library 2.0 Certificate #3060 listed on the cryptographic module validation program (CMVP) website.

For more information, please refer to Commvault Books Online: Software Encryption.

3.2.2 Hardware Encryption and Key Management

All MediaAgents are supporting hardware encryption, 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.
LTO-4 tape drives or higher provide the necessary controls to the backup applications to get the encryption capabilities as well as set the encryption properties on the drive. Some tape libraries like the ETERNUS LT also provide key management services. Commvault's Hardware Encryption feature provides key management for the tape libraries that do not support key management by themselves.

Key Management for Hardware Encryption can be enabled in one of the two ways:

- 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. Commvault software generates a different random 128 or 256 key for every data chunk it writes. Each job can contain multiple chunk, so each backup job can have multiple randomly generated keys. With multiple different keys the strength of the encryption is very high. The Key is encrypted and stored in the CommServe database.

When data chunks are pruned (erased), the database entry and the associated key for that data chunk is deleted. Open keys in memory are deleted using memset().

- Hardware or Library Managing the Encryption Keys
  Some tape libraries like ETERNUS LT140 / LT260 also provide key management services.
  If you have an enabled hardware vendor license applied on the library for key management, 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, such as the tape library and tape drive.

For more information, please refer to Commvault Books Online: Commvault Management of Encryption keys.

3.3. Veritas NetBackup

3.3.1 NetBackup security and encryption

NetBackup security and encryption provide protection for all parts of NetBackup operations on NetBackup master servers, media servers, and attached clients. Also made secure are the operating systems on which the servers and clients are running.
The backup data is protected through encryption processes and vaulting. NetBackup data that is sent over the network is protected by dedicated and secure network ports.

3.3.2 Key Management

- About the Key Management Service (KMS)

The NetBackup Cryptographic Module is FIPS validated (FIPS: Federal Information Processing Standards).
NetBackup Key Management Service (KMS) uses the NetBackup Cryptographic Module and can now be operated in FIPS mode.
The NetBackup 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.

KMS 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 and runs on Windows and UNIX. KMS generates keys from your passcodes or it auto-generates keys. The KMS operations are done through the KMS command line interface (CLI) or the Cloud Storage Server Configuration Wizard (when KMS is used with Cloud storage providers).

- Configuration of KMS

The configuration of KMS is done by creating the key database, key groups, and key records.
The steps to configure and initialize KMS are:

- Create the key database, the host master key (HMK), and the key protection key (KPK):

An empty key database is created by invoking the service name with the *-createemptydb* option. This process checks and ensures that an existing key database does not already exist, and then proceeds with the creation.
The initialization process of the KMS creates the two protection keys – the Host Master Key (HMK) and the Key Protection Key (KPK).

- Create a key group that matches the volume pool:

A key group is a logical collection of key records where no more than one record is in the active state. The key group definition consists: name (must have the prefix *ENCR_*), tag, cipher, description, creation time, last modification time.
Command to create the key group ‚mygroup': `nbkmsutil -createkg -kgname ENCR_mygroup`

- Create an active key record:

A key record consists of the following critical pieces of information: name, key tag, key group tag, state, encryption key, description, creation time, last modification time.
The active key record can either be created in the prelive state and then transferred to the active state or directly in the active state.

- Configuring NetBackup to work with KMS

The first step in configuring NetBackup to work with KMS is to set up a NetBackup-supported, encryption-capable tape drive and the required tape media.
The second step is to configure NetBackup as you would normally, except that the encryption-capable media must be placed in a volume pool with the identical name as the key group you created when you configured KMS.
Note: The Key Management feature requires the key group name and NetBackup volume pool name match identically and both with *ENCR_* prefix. This method of configuration-enabled encryption support requires no major changes to the NetBackup system management infrastructure.

3.3.3 Using KMS for encryption

You can use KMS to run an encrypted tape backup, verify an encrypted tape backup, and manage keys. The following topics provide examples for each of these scenarios:

- Importing KMS encrypted images

Importing KMS encrypted images is a two-phase operation.

- In phase 1, the media header and each fragment backup header is read. This data is never encrypted and does not require a key. However, the backup headers indicate if the fragments file data is encrypted with KMS or not.
- Phase 2 rebuilds the catalog *.f* file, which requires it to read the encrypted data. The key-tag (KAD in SCSI terms) is stored on the tape by the hardware. The NetBackup tape management process (bptm) reads the key-tag from the drive, and sends it to KMS for a key lookup. If KMS has a key, then the phase 2 process continues to read the encrypted data. If KMS has no key, the data is not readable until the KMS has the key recreated by using the pass phrase.

If you do not destroy keys, then KMS contains all the keys ever used and you can import any encrypted tape. Moving the keystore to the DR site avoids the need of recreation!

■ Running an encrypted tape backup

To run an encrypted tape backup, you must have a policy that is configured to draw from a volume pool with the same name as your key group.

■ 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.

More information and considerations that relate to the functionality and use of KMS, see: Veritas NetBackup™ Security and Encryption Guide NBU 8.1.2, chapter 9: Data at rest key managment (Last Published:2018-10-16).

4. Key Management via Tape Library

4.1. General Overview

Some tape libraries like ETERNUS LT also provide key management services within the tape library by using the hardware encryption function provided by LTO tape drives to manage encryption keys on the tape library.
The library generates, manages and stores the encryption keys per tape cartridge and the tape drive encrypts the data without the expense of a backup software license or the need of an additional server for the encryption key management. Therefore, every backup job written to a specific tape media will have the same key.
The Key Management Function enables easy construction of a secure backup system independently of the operating system and backup software, since the tape library will automatically handle encryption and key management.
Note: The encryption and key management function of the backup software must be disabled.

4.2. Key Management via ETERNUS LT

4.2.1 Key types

The Key Management Function uses two types of keys for encryption: the master key and the encryption key.

■ A master key is set for each tape library respectively for each logical library (or partition) and is invisible to users. The master key can be manually created using arbitrary characters or automatically generated using the tape library.
Each tape library automatically generates a master key based on data unique to the tape library. For this reason, other tape libraries cannot generate the same master key.

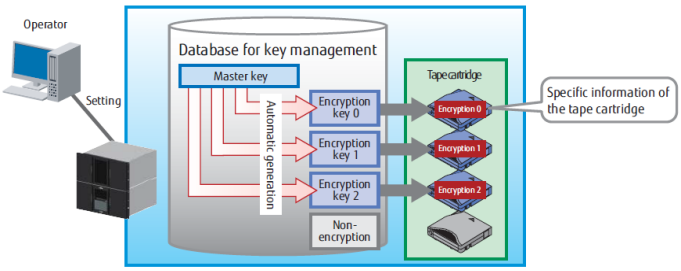


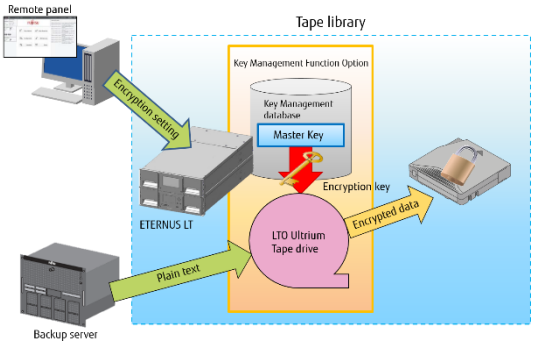
Figure 2: Automatic generation of keys

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

■ The encryption key is assigned to each data cartridge during the data write process. Different data cartridges never have the same encryption key because the tape library automatically generates an encryption key based on the master key and data unique to each data cartridge.
If different tape libraries have the same master key and same data unique to the data cartridge, the libraries will generate the same encryption key for the cartridge.

■ Although the information of the master and encryption key and encryption setting information are stored redundantly in the database of the tape library. In addition, Fujitsu recommends exporting the keys (to a binary file) and keeping in a safe place to guarantee the reading of the encrypted data in case the tape library fails.

4.2.2 How the Key Management Function works:



The Key Management Function Option allows the use of the encryption function provided by Ultrium tape drives to manage encryption keys on the tape library. The Key Management Function Option applies the encryption settings from the remote panel to the tape library and assigns the master key. The encryption key that is automatically generated for each data cartridge by the tape library is based on the master key, and this information is stored in a database in the tape 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 is invisible to users.

Figure 3: Process of Key Management via ETERNUS LT

The optional Key Management Function requires a separate key management license for the appropriate ETERNUS LT library.

4.3. Usage Scenarios

■ Data Sharing between Centers

Setting the same master key for multiple tape libraries installed in the same center or separate centers enables these libraries to share data cartridges with encryption keys hidden from view.

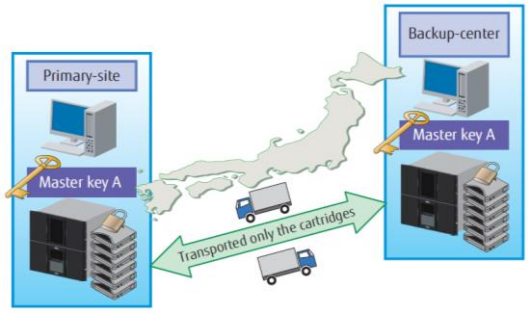
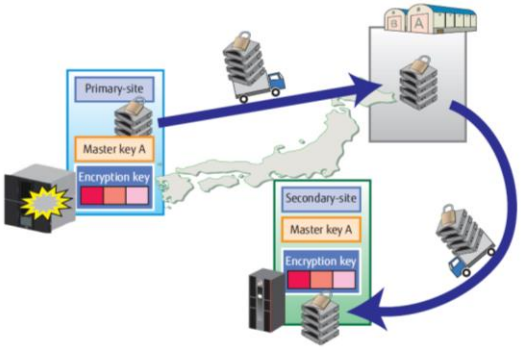


Figure 4: Data cartridge sharing using one master key

■ Encryption of Data Cartridges Stored at an External Location



For disaster recovery, encrypted data cartridges can be stored at an external location and, when needed, brought back to read the data on them. Even if a data cartridge in storage is lost or stolen, the encryption can prevent data leakage.
Once a data cartridge in storage is inserted into its original tape library or one with the same master key, the data can be read from the library without setting the key again.
Note: Once encryption keys are exported, even if the tape library becomes unavailable such as in the event of a disaster, data on the data cartridge can be read by importing the encryption key to a tape library with a different master key.

Figure 5: External storage of data cartridges

■ Encryption of Each Logical Library (or Partition)

The partitioning option divides one ETERNUS LT library in several logical libraries. The library software generates and assigns a single and unique master key for each logical ETERNUS LT library (or partition).
The library administrator can configure encrypted/unencrypted settings for each tape cartridge and each logical library via the central ETERNUS LT remote management console. In addition, he can ensure the security of the library, without the intervention of the backup operator.

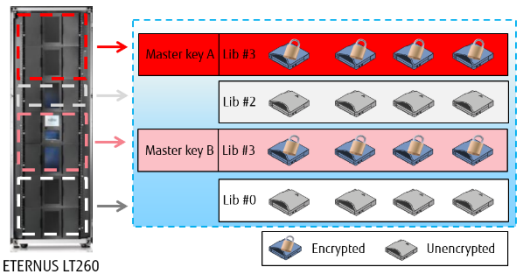


Figure 6: Encryption of logical library

For more details, see the User Guide: ETERNUS LT Key Management Function Option.

5. Key Management Interoperability Protocol (KMIP®)

5.1. KMIP Standard

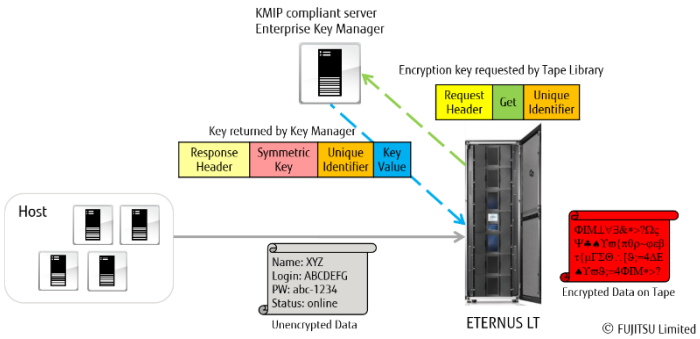
The Key Management Interoperability Protocol (KMIP®) is a specification developed by OASIS®. The first version of KMIP was formally ratified on October 2010. Its function is to standardize communication between enterprise key management systems and encryption systems.

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.

5.2. KMIP with ETERNUS LT

The Fujitsu Storage ETERNUS LT140 and ETERNUS LT260 tape systems support the 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 that it needs to use 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, that allow the storage system to be sure it is receiving the correct key. Headers for both the request and response provide information such as the protocol version and message identifiers that the participating systems can use to track and correlate the messages.

The KMIP key management functionality requires a separate license for the appropriate ETERNUS LT library.

The KMIP implementation of ETERNUS LT140 and 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

6. Index of Figures

Contact
Fujitsu Technology Solutions GmbH
Mies-van-der-Rohe-Str. 8
80807 Munich, German
E-mail: storage-pm@ts.fujitsu.com
Website: www.fujitsu.com/eternus
2019-01-14 WW EN