LTO4 Hardware Encryption Best Practices

By Vic Ludlam
Distributed by Dynamic Solutions International

dsi dynamic solutions international

Contents

Information in this document is subject to change without notice.

For more information please contact DSI directly at 800-641-5215 or sales@dynamicsolutions.com

Section 1

Overview

Some DSI LTO4 tape systems provide for an optional Hardware Encryption Kit, these are the DSIxxxx. This kit allows the LTO4 tape unit itself to encrypt data written to tape, thereby avoiding host-based encryption software and overhead. The LTO4 tape units utilize an onboard USB port that can accept a USB hardware encryption device, commonly called a 'Key Server Token'. The Key Server Token looks very similar to a common USB drive. However, only an LTO4 tape unit can access the encryption keys contained within a Key Server Token device. The basic process is that one LTO4 tape unit, having the Key Server Token installed, will encrypt the tape data using the most recent key available on the device. A remote LTO4 tape unit at a disaster recovery location, using a copy of the Key Server Token, can decrypt the tape data at that location.

The remainder of this document outlines the suggested 'best practices' from Dynamic Solutions International, after careful and thorough testing of the product. In every case, the client should review the Encryption User Guide included with the Hardware Encryption Kit, to become familiar with the hardware encryption methodology, and determine the best usage for the client's individual needs.

Section 2

Hardware Components

The Hardware Encryption Kit contains the following components for each LTO4 drive ordered with the option:

1. Two Key Server Tokens
2. A bag of holders and identification cards
3. Product Documentation

The second Key Server Token is intended as a backup for the first token.

Drive Firmware Requirements

If an LTO4 tape unit is ordered from DSI with the Hardware Encryption Kit, DSI ensures that the unit will have the proper firmware levels installed to use hardware-based encryption upon delivery. If hardware encryption is ordered as an add-on to an existing LTO4 installation, firmware changes may be required to your unit to utilize hardware encryption. Contact DSI Support to ensure your unit has the correct firmware levels to support hardware encryption.

Section 3

Hardware Encryption Basic Recommendations

In order to use LTO4 Hardware Encryption, each LTO4 tape unit that will be encrypting tapes requires an IP connection. The LTO4 units have a built-in GUI Interface that provides management and control of keys on the Key Server Token. Configure the IP connection for the LTO4 tape unit as specified in the LTO4 installation documentation.

Once a Web Browser can access the LTO4 tape unit, Key Management is accessed via the Security tab. The first task is to assign a PIN to a new Key Server Token. Remember and record this PIN; it requires at least 8 characters, must contain at least one capital letter, and 2 numeric digits. If a key is lost or a key can not be matched to an encrypted tape, the data can no longer be retrieved. DSI recommends that each Key Server Token use the same PIN for the intended Production key, and the associated backup or Disaster Recovery (DR) key to avoid confusion. The PIN for the Key Server Tokens should be recorded and stored in a secure location separate from the Key Server Tokens themselves.

Each Key Server Token can hold 100 individual encryption keys. You cannot delete keys on the Key Server Token. If the Key Server Token becomes full, you must purchase new Key Server Tokens. DSI recommends that new Key Server Tokens be purchased in pairs (for each LTO4 unit that will be using hardware encryption) to replace the full key Server Tokens. Full Key Server Tokens *MUST* be retained for the life of the earliest tape encrypted by the Key Server Token.

When encrypting a tape, the LTO4 unit will use the most recent encryption key created on the Key Server Token. The client should ensure that the backup Key Server Token always has the latest encryption key in order to ensure a given tape can be decrypted.

Section 4

Recommended Key Server Token Management

The Key Server Token simplifies encryption and decryption of tapes. If a tape has been encrypted via Hardware Encryption, decryption of that tape will occur automatically, provided that the decrypting LTO4 unit has an up-to-date copy of the Key Server Token that created the tape.

As well, the key records on a Key Server Token can be backed up to a PC file, on the PC that is running the LTO4 GUI interface program. The following are DSI 'Best Practices' in managing the Key Server Tokens:

1. Each Hardware Encryption Kit contains two Key Server Tokens. Keep one Key Server Token with the Primary LTO4 Unit and the second key with the Disaster Recovery site unit. If there is no DR site, keep the second key in a location other than the primary site.

2. For sites that have multiple LTO4 tape units in operation, mark each Key Server Token with the Host Unit number creating the encrypted tapes. Do *NOT* attempt to use a single Key Server Token between multiple LTO4 tape units. If the client has their own DR site, it would be ideal to have the tape unit numbers at the DR site match the tape unit numbers at the Production site, this will help avoid confusion.

3. Use the manual method to generate new keys on a given Key Server Token. DSI does not recommend using the 'automatic' method of generating new keys on a Key Server Token at periodic intervals. The problem with this method is that the LTO4 drive itself does not have NTP (Network Time Protocol) capability, and a drive in one location could automatically create a new encryption key that would appear to be later than the decryption key at a remote location.

4. The client should generate a new key at the beginning of each month. Since most clients have special month-end procedures, this action can easily be added to current month-end processes. Many auditors will accept a once-per-month creation of a unique

encryption key (check with your own auditor). Given this key generation strategy, a 100 Key Server Token will last for 8 years.

5. Once a new key is generated on the Key Server Token at the Production site, update the Secondary Key Server Token as soon as possible. DSI recommends that this be accomplished by copying the Primary Key Server Token file to a laptop. Next, move that laptop to the Secondary site, and upload the file to the Secondary Key Server Token. This avoids having both Key Server Tokens in the same location at the same time.

6. For obvious security reason we recommend never transporting a given encrypted tape with its USB Key Server Token!

Section 5

Key Server Token Storage

Remember, if your institution requires permanent retention of data, you must permanently retain the Key Server Token as well. DSI recommends that if some client tapes require very long-term/permanent storage, a client might want to use separate hardware encryption Key Server Tokens for long-term archive. When considering long-term encrypted storage requirements, consider DSI as your consultant to maximize storage protection, minimize storage costs, and provide the best storage solution for your environment.

Section 6

Procedures in a Banking Environment

Banks have auditing requirements that will mandate a consistent rotational key management procedure. Below is a suggested key management procedure and key usage for the banking environment. This is intended to be applied to each LTO tape unit is use.

Initial Key Server Token Setup

1. Begin encryption with a new Key Server Token, creating the Key Server Token with a unique PIN and the first encryption key. Mark the tag of the Key Server Token with the date of the first day the Key server Token is placed in service.
2. Back up the Key Server Token by exporting the Key Server Token contents to a PC file.
3. Create the second Key Server Token with the same PIN as the Primary Key Server Token. Update the second Key Sever Token by importing the PC file from the backup of the Primary Key Server Token. Do *NOT* simply create a token on the second Key Server Token! - that key will not match. Mark the tag of the Key Server Token with the same date as the date of the first day the primary Key Server Token is placed in service.
4. Move the second Key Server Token to the Disaster Recovery site. If there is no DR site, move the key to a secure off-site location.

Key Server Token Usage

1. Encrypt all tapes on the Production LTO4 unit(s). Use the previous movement/rotation procedures to move tapes to the Disaster Recovery site or off-site storage. Leave the Key Server Token in the LTO4 unit
2. At the completion of month-end processing and creation of all output tapes, create a new key on the Key Server Token. Do not rely on the automated key creation method.
3. Once the next month's key is generated, update the backup Key Server Token by backing up the keys on the Primary

Token, and using that file to update the backup Key Server Token.

Key Server Token Retirement

1. A key Server Token can hold up to 100 keys. Updating the key on the Key Server Token each month allows the Key Server Token to hold over 8 years of keys. If monthly key rotation is in use, DSI recommends that a given key be retired around the 7-year usage mark, and retirement is coterminous with the institutions fiscal year end. This avoids confusion when determining what Key Server Token is required to decrypt historical tape records. The following procedure should be used to retire a pair of Key Server Tokens:

    a. Remove the Key Server Token from service at the end of the fiscal year processing, after ensuring that the Primary and Secondary Key Server token have the same keys.

    b. Mark the tag of the Primary and Secondary Key Token Servers with the fiscal year-end date of processing.

    c. Retain the primary Key Server Token for at least 4 months on-site, and move the Secondary Key Server Token to the DR site, or a secure off-site location. The Primary Key Server Token is retained at the production site to ensure timely retrieval of year-end data or post-processing any client requests for tax information.

    d. At the end of the 4-month on-site period, move the Primary key to an off-site location. Ideally, this would be held in a different location than the secondary key.

    e. Create the new Key Server Tokens for the next period as shown in step 1 above.

Section 7

Alternate Key Rotation Suggestions

Some financial institutions may require different key rotation policies based upon auditor requirements. The following suggestions are alterations to the example above, where DSI suggested that a new key be generated once-per-month.

Weekly Encryption Requirements

If weekly encryption key changes are mandated, DSI recommends that each LTO4 unit have a new Key Server Token pair purchased each fiscal year. The first set of Key Server Tokens would be used until the fiscal year-end of the financial institution. Every Key Server Token pair after that point will only be used for that fiscal year, and retires (as described above) after the completion of year-end processing. New Key Server Token pairs should be purchased at least two months before the bank fiscal year-end for each LTO4 unit in use.

Section 8

Alternative Usage for Mortgage Companies & Savings and Loans

Mortgage companies, as well as many banking institutions that supply long-term loans via contract may require storage of data for long periods of time. The modifications below to the above examples may be beneficial for those institutions that require long-tem retention of data.

1. For each LTO4 drive, purchase four (4) Key Server Tokens. These Key Server Tokens are broken down to (2) Primary/backup Tokens for short-tem retention, and (2) Long-term Retention Key Server Tokens.
2. Follow the basic example above. However the PIN for the long-term retention Key Server Tokens should be different from the short-term retention Key Server Tokens.
3. Whenever a long-term tape is created, only the long-term Key Token Server is used to encrypt these tapes. This pair of Key Server Tokens will typically have a new key generated on the Key Server Token pair at fiscal year-end.
4. All temporary tapes utilize the short-term Key Server Tokens during normal operations. Once the short-term Key Server Tokens are full, the short-term Key Server Tokens can be destroyed after the expiration of the last tape encrypted by the last key on the short-term Key Server Token.

A client may elect to use a dedicated LTO4 drive for long-term retention tapes, and different drives for short-term retention tapes. In this case, most backups would be directed to the 'short-term retention drive' (using the short-term Key Server Token). Long-term data would be recorded to the dedicated LTO4 drive that uses the long-term Key Server Tokens. While this helps eliminate operator error in changing Key Server Tokens, it doubles the cost of hardware to dedicate certain tape units to 'short-term' vs. 'long-term' storage encryption. Each client will have unique requirements that will dictate the most cost-effective solution for their operation.

DSI does provide consulting services to help you determine the most cost-effective implementation for your environment. For further questions regarding personal consultation, contact you local DSI Sales Representative, or your local Unisys Sales Representative.