IBM LTO Generation 5 Encrypting Tape Drive

Security Policy

Version 1 Revision 2

1 Document History 1

2 Introduction 2

2.1 References 3
2.2 Document Organization 3

3 LTO Generation 5 Encrypting Tape Drive Cryptographic Module Description 4

3.1 Overview 4
3.2 Secure Configuration 6
3.3 Ports and Interfaces 9
3.4 Roles and Services 11
3.5 Physical Security 17
3.6 Cryptographic Algorithms and Key Management 18
3.7 Design Assurance 21
3.8 Mitigation of other attacks 21

1 Document History

Date	Author	Change
06/02/2010	Said Ahmad	Initial Creation
07/22/2010	Said Ahmad	Updated per SAIC comments
10/27/2010	Said Ahmad	Update EC numbers
03/11/2011	Said Ahmad	Updates per SAIC comments

2 Introduction

This non-proprietary security policy describes the IBM LTO Generation 5 Encrypting Tape Drive cryptographic module and the approved mode of operation for FIPS 140-2, security level 1 requirements. This policy was prepared as part of FIPS 140-2 validation of the LTO Gen5. The LTO Gen5 Encrypting Tape Drive is referred to in this document as the LTO Gen5, the IBM LTO Gen5, and the encrypting tape drive.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2—*Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the NIST web site at:

http://csrc.nist.gov/groups/STM/cmvp/

The security policy document is organized in the following sections:

- Introduction
- References
- Document Organization

LTO Gen5 Encrypting Tape Drive Cryptographic Module Description

- Cryptographic Module Overview
- Secure Configuration
- Cryptographic Module Ports and Interfaces
- Roles and Services
- Physical Security
- Cryptographic Key Management
- Self-Tests
- Design Assurance
- Mitigation of Other Attacks

2.1 References

This document describes only the cryptographic operations and capabilities of the LTO Gen5 Encrypting Tape Drive. More information is available on the general function of the LTO Gen5 Encrypting Tape Drive at the IBM web site:

http://www.ibm.com/storage/tape/

The tape drive meets the T10 SCSI-3 Stream Commands (SSC) standard for the behavior of sequential access devices.

The LTO Gen5 Encryption Tape Drive supports 2 host interface types: Fibre channel (FC) and serial-attached SCSI (SAS). The physical and protocol behavior of these ports conforms to their respective specifications. These specifications are available at the INCITS T10 standards web site:

http://www.T10.org /

A Redbook describing tape encryption and user configuration of the LTO Gen5 drive in various environments can be found at:

http://www.redbooks.ibm.com/abstracts/sg247320.html?Open

The LTO Gen5 drive format on the tape media is designed to conform to the IEEE P1619.1 committee draft proposal for recommendations for protecting data at rest on tape media. Details on P1619.1 may be found at:

http://ieeexplore.ieee.org/servlet/opac?punumber=4413113

2.2 Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the submission package contains:

- Vendor Evidence Document
- Other supporting documentation and additional references

With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Documentation is proprietary to IBM and is releasable only under appropriate non-disclosure agreements. For access to these documents, contact IBM.

3 IBM LTO Generation 5 Encrypting Tape Drive Cryptographic Module Description

3.1 Overview

The IBM LTO Generation 5 Encrypting Tape Drive, also referred to herein the LTO Gen5 Encrypting Tape Drive and the module, is a set of hardware, firmware, and interfaces allowing the optional storage and retrieval of encrypted data to magnetic tape cartridges. The entire "brick" unit of the LTO Gen5 tape drive is FIPS certified as a multi-chip, standalone cryptographic module. In customer operation the "brick" unit may be used in conjunction with a computer system or tape library. Block diagrams of the LTO Gen5 Encrypting Tape Drive are shown below:

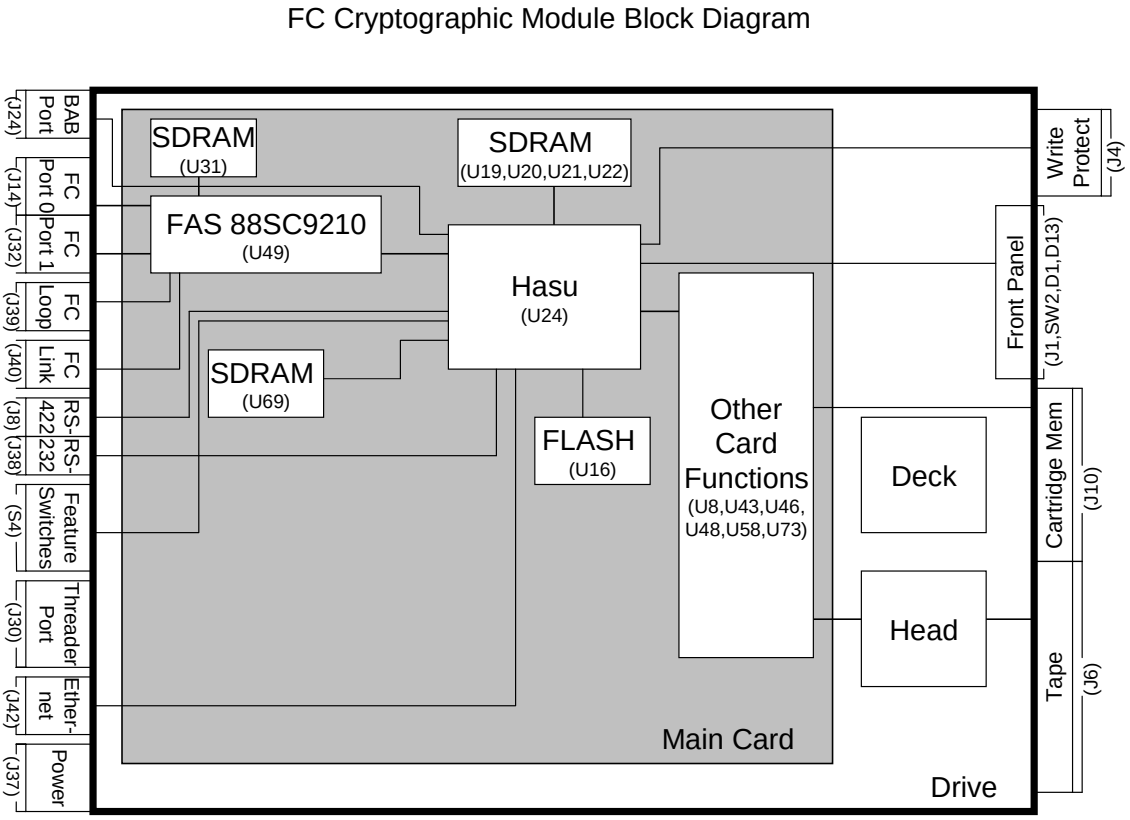


Figure 1a: LTO Gen5 Fibre Channel Drive Block Diagram

SAS Cryptographic Module Block Diagram

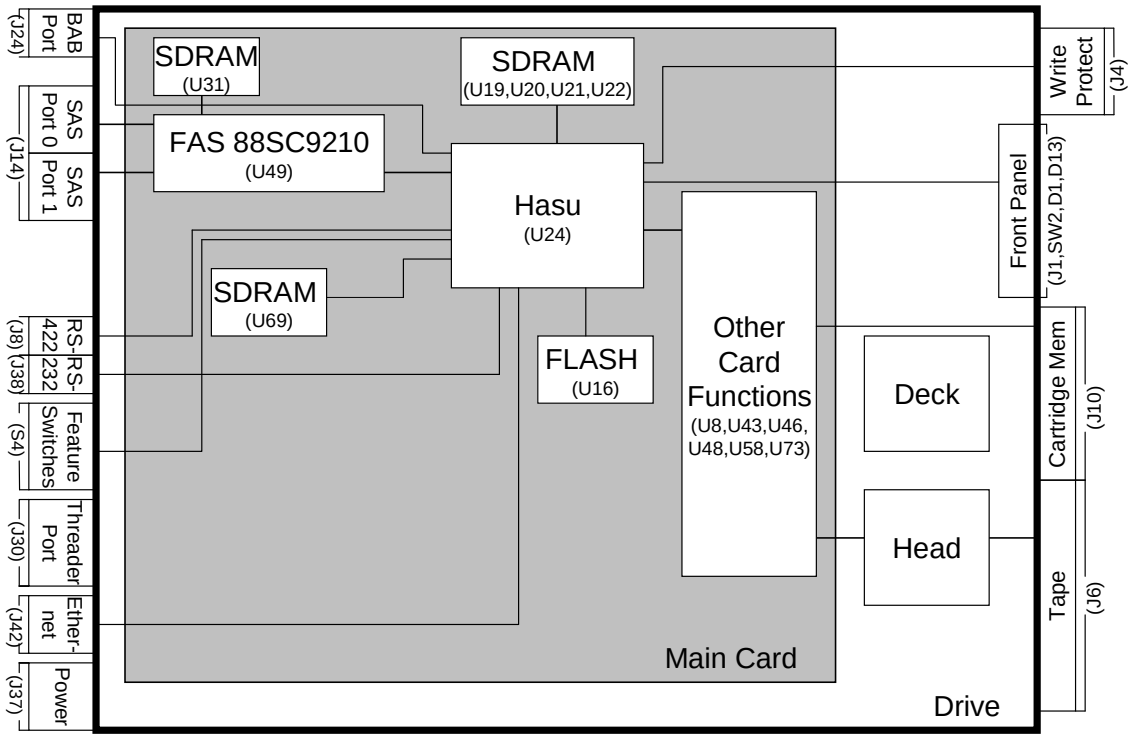


Figure 1b: LTO Gen5 SAS Drive Block Diagram

The LTO Gen5 Encrypting Tape Drive has two major cryptographic functions:

- Data Block Cipher Facility: The tape drive provides functions which provide the ability for standard tape data blocks as received during SCSI-type write commands to be encrypted before being recorded to media using AES-GCM block cipher using a provided key, and decrypted during reads from tape using a provided key.
    - Note the AES-GCM block cipher operation is performed after compression of the host data therefore not impacting capacity and data rate performance of the compression function
    - The LTO Gen5 drive automatically performs a complete and separate decryption and decompression check of host data blocks after the compression/encryption process to validate there were no errors in the encoding process
- Secure Key Interface Facility: The tape drive provides functions which allow authentication of the tape drive to an external IBM key manager, such as the IBM Encryption Key Manager (EKM) or the Tivoli Key Lifecycle Manager (TKLM), and allow transfer of protected key material between the key manager and the tape drive.

3.2 Secure Configuration

This section describes the approved mode of operation for the LTO Gen5 drive to maintain FIPS-140 validation.

There are two configurations for the LTO Gen5 in the approved mode of operation. They are:
- System-Managed Encryption (SME)
- Library-Managed Encryption (LME)

In order to be in an approved mode of operation, the values of the fields Key Path (manager Type) (from VPD), In-band Key Path (Manager Type) Override, Indirect Key Mode Default, Key Scope, and Encryption Method must be set according to the table below. More details can be found in the LTO Ultrium Tape Drive SCSI Reference.

Table 1: Settings for Approved Modes of Operation

Required Fields	System-Managed Encryption (SME)	Library-Managed Encryption (LME)
Key Path (Manager Type) (from VPD) Mode Page X'25', byte 21, bits 7-5	X'1'	X'6'
In-band Key Path (Manager Type) Override Mode Page X'25', byte 21, bits 4-2	X'0' or X'1'	X'0'
Indirect Key Mode Default Mode Page X'25', byte 22, bit 4	B'0'	B'0'
Key Scope Mode Page X'25', byte 23, bits 2-0	X'0' or X'1'	X'0' or X'1'
Encryption Method Mode Page X'25', byte 27	X'10' or X'1F'	X'60'

A user can determine if the LTO Gen5 is in the approved mode of operation by issuing a SCSI Mode Sense command to Mode Page X'25' and evaluating the values returned.

Certain commands are prohibited while in the approved modes of operation. The commands vary based on which configuration is used in the approved mode. In the LME configuration, all Mode Select commands to subpages of Mode Page X'25' are prohibited. In the SME configuration, Mode Select commands to the following subpages of Mode Page X'25' are prohibited.

Table 2: Mode Select Eligibility of Mode Page X'25' Subpages

Mode Page X'25' Subpages	System-Managed Encryption (SME)	Library-Managed Encryption (LME)
X'C0' – Control/Status	**Allowed**	Prohibited
X'D0' – Generate dAK/dAK' Pair	Prohibited	Prohibited
X'D1' – Query dAK	Prohibited	Prohibited
X'D2' – Update dAK/dAK' Pair	Prohibited	Prohibited
X'D3' – Remove dAK/dAK' Pair	Prohibited	Prohibited
X'D5' – Drive Challenge/Response	**Allowed**	Prohibited
X'D6' – Query Drive Certificate	**Allowed**	Prohibited
X'D7' – Query/Setup HMAC	Prohibited	Prohibited
X'D8' – Install eAK	Prohibited	Prohibited
X'D9' – Query eAK	Prohibited	Prohibited
X'DA' – Update eAK	Prohibited	Prohibited
X'DB' – Remove eAK	Prohibited	Prohibited
X'DF' – Query dSK	**Allowed**	Prohibited
X'E0' – Setup SEDK	**Allowed**	Prohibited
X'E1' – Alter DKx	**Allowed**	Prohibited
X'E2' – Query DKx (Active)	**Allowed**	Prohibited
X'E3' – Query DKx (Needed)	**Allowed**	Prohibited
X'E4' – Query DKx (Entire)	**Allowed**	Prohibited
X'E5' – Query DKx (Pending)	**Allowed**	Prohibited
X'EE' – Request DKx (Translate)	**Allowed**	Prohibited
X'EF' – Request DKx (Generate)	**Allowed**	Prohibited
X'FE' – Drive Error Notify	**Allowed**	Prohibited

Loading a FIPS 140-2 validated drive microcode level and configuring the drive for SME or LME operation initializes the LTO Gen5 into the approved mode of operation.

The LTO Gen5 supports multi-initiator environments, but only one initiator may access cryptographic functions at any given time. Therefore the LTO Gen5 does not support multiple concurrent operators.

The LTO Gen5 implements a non-modifiable operational environment which consists of a firmware image stored in FLASH. The firmware image is copied to, and executed from, RAM. The firmware image can only be updated via FIPS-approved methods that verify the validity of the image.

The LTO Gen5 drive operates as a stand-alone tape drive and has no direct dependency on any specific operating system or platform for FIPS approved operating mode, but does have requirements for:

- Key Manager/Key Store attachment
- Drive Configuration

The following criteria apply to the usage environment:

- Key Manager and Key Store Attachment
  - In both SME and LME modes of operation, an IBM key manager, such as the Encryption Key Manager (EKM) or the Tivoli Key Lifecycle Manager (TKLM), and a supported key store must be used in a manner which supports secure import and export of keys with the LTO Gen5 drive :
    - Keys must be securely passed into the LTO Gen5 drive. The key manager must support encryption of the Data Key to form an Session Encrypted Data Key (SEDK) for transfer to the LTO Gen5 drive using the LTO Gen5 drive public Session Key and a 2048-bit RSA encryption method.
    - The key manager/key store must be able to use the DKi it supplies the drive to determine the Data Key.

- Drive Configuration requirements
  - The LTO Gen5 drive must be configured in SME or LME encryption mode.
  - The LTO Gen5 drive must have the FIPS 140-2 validated drive firmware level loaded and operational.
  - Drive must be configured in the approved mode of operation.
  - In LME mode, the LTO Gen5 drive must be operated in an automation device which operates to the LDI or ADI interface specifications provided.

3.3 Ports and Interfaces

The cryptographic boundary of the LTO Gen5 drive cryptographic module is the drive brick. Tape data blocks to be encrypted (write operations) or decrypted data blocks to be returned to the host (read operation) are transferred on the host interface ports using SCSI commands, while protected key material may be received on the host interface ports or the library port.

The physical ports are separated into FIPS-140-2 logical ports as described below.

Table 3: Ports Common to All Host Interface Types

LTO Gen5 Drive Physical Ports	**FIPS-140-2 Logical Interface**	**Crypto Services**	**Interface Functionality**
BAB Port	Disabled	None	▪ Disabled by FIPS approved firmware levels.
RS-422 Port	Data Input Data Output Control Input Status Output	Yes	▪ Inputs data ▪ Crypto: Inputs protected keys from the key manager in LME mode. ▪ Outputs data ▪ Outputs encrypted key components ▪ Inputs LDI and LMI protocol commands. ▪ Outputs LDI and LMI protocol status.
RS-232 Port	Disabled	None	▪ Disabled by FIPS approved firmware levels.
Ethernet Port	Control Input Status Output Data Input	None	▪ Inputs controls and image for firmware load ▪ Outputs status
Threader Power Port	Power	None	▪ Supplies power to threader unit internal to tape drive brick.
Input Power Port	Power	None	▪ Inputs power to the LTO Gen5 drive
Write Protect Switch	Control Input	None	▪ Inputs write protect state of the cartridge
Front Panel Single-Character Display (SCD)	Status Output	None	▪ Displays status
Front Panel Amber LED	Status Output	None	▪ Displays status
Front Panel Green LED	Status Output	None	▪ Displays status
Front Panel Unload Button	Control Input	None	▪ Inputs unload command ▪ Places the drive in manual diagnostic mode ▪ Scrolls through manual diagnostics ▪ Exits manual diagnostic mode ▪ Forces drive dump ▪ Resets the drive
Cartridge Memory RFID Port	Data Input Data Output	Yes	▪ Inputs parameters. ▪ Crypto: Inputs external key structures ▪ Outputs parameters. ▪ Crypto: Outputs external key structures
Read/Write Head	Data Input Data Output Control Input	None	▪ Inputs data from tape cartridges ▪ Outputs data to tape cartridges ▪ Inputs command to load firmware from special FMR cartridges

Table 4a: Fibre Channel-Specific Host Interfaces Ports

LTO Gen5 FC Drive Physical Ports	**FIPS-140-2 Logical Interface**	**Crypto Services**	**Interface Functionality**
Fibre Channel Port 0 Fibre Channel Port 1	Data Input Data Output Control Input Status Output	Yes	▪ Inputs data ▪ Crypto: Inputs protected keys from the key manager in SME mode. ▪ Outputs data ▪ Outputs encrypted key components ▪ Inputs SSC-3 SCSI protocol commands ▪ Outputs SSC-3 SCSI protocol status
Fibre Channel Loop ID Port	Control Input Status Output	None	▪ Inputs fibre channel interface control parameters ▪ Outputs fibre channel interface status
Fibre Channel Link Characteristics Port	Control Input	None	▪ Inputs fibre channel interface control parameters
Feature Switches	Control Input	None	▪ Inputs RS-422 interface control parameters ▪ Inputs fibre channel interface control parameters ▪ Inputs read/write head cleaner brush control parameters

Table 4b: SAS-Specific Host Interfaces Ports

LTO Gen5 SAS drive Physical Ports	**FIPS-140-2 Logical Interface**	**Crypto Services**	**Interface Functionality**
SAS Connector	Data Input Data Output Control Input Status Output Power	Yes	▪ Inputs data ▪ Crypto: Inputs protected keys from the key manager in SME mode ▪ Outputs data ▪ Outputs encrypted key components ▪ Inputs T10 SAS Standards commands ▪ Outputs T10 SAS Standards status
Feature Switches	Control Input	None	▪ Inputs RS-422 interface control parameters ▪ Inputs read/write head cleaner brush control parameters

3.4 Roles and Services

The LTO Gen5 drive supports both a Crypto Officer role and a User role, and uses basic cryptographic functions to provide higher level services. For example, the LTO Gen5 drive uses the cryptographic functions as part of its data reading and writing operations in order to perform the encryption/decryption of data stored on a tape.

The Crypto Officer role is implicitly assumed when an operator performs key zeroization. The User role is implicitly assumed for all other services.

The two main services the LTO Gen5 drive provides are:

- Encryption or decryption of tape data blocks using the Data Block Cipher Facility.
- Establishment and use of a secure key channel for key material passing by the Secure Key Interface Facility.

It is important to note that the Secure Key Interface Facility may be an automatically invoked service when a user issues Write or Read commands with encryption enabled that require key acquisition by the LTO Gen5 drive. Under these circumstances the LTO Gen5 drive automatically establishes a secure communication channel with a key manager and performs secure key transfer before the underlying write or read command may be processed.

3.4.1 User Guidance

The services table describes what services are available to the User and Crypto Officer roles.

- There is no requirement for accessing the User Role
- There is no requirement for accessing the Crypto Officer Role

Single Operator requirements:

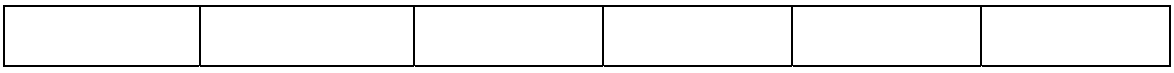
- The LTO Gen5 drive enforces a requirement that only one host interface initiator may have access to cryptographic services at any given time.

3.4.2 Provided Services

Available services are also documented in the specified references. They are summarized here:

Table 5: Provided Services

Service	Interface(s)	Description	Inputs	Outputs	Role
General SCSI commands	- Host	As documented in the LTO Ultrium Tape Drive SCSI Reference	See description	See description	User
General Library Interface commands	- Library	As documented in the Drive Library LDI and LMI Interface Specifications	See description	See description	User
Unload tape	- Host/Library - Front Panel Unload Button	Unload tape can be performed using unload button or via commands over the host or library interrface	Button press	Green LED flashes while unload is in progress.	User
Enter manual diagnostic mode	- Front Panel Unload Button	Place in manual diagnostic mode via the unload button	Button press	SCD displays 0. Amber LED becomes solid.	User
Scrolls through manual diagnostic functions	- Front Panel Unload Button	Scroll through manual diagnostic functions via the unload button	Button press	SCD changes to indicate scrolling.	User
Exits manual diagnostic mode	- Front Panel Unload Button	Exit manual diagnostic mode via the unload button	Button press	SCD becomes blank. Green LED becomes solid.	User
Forces drive dump	- Front Panel Unload Button	Force a drive dump via the unload button	Button press	SCD shows 0, then becomes blank.	User
Resets the drive	- Front Panel Unload Button	Power-cycle the device via Unload Button	Button press	Reboot occurs.	User



Service	Interface(s)	Description	Inputs	Outputs	Role
Encrypting Write-type Command	- Host	The Secure Key Interface Facility automatically requests a key, provides authentication data, securely transfers and verifies the key material. The Data Block Cipher Facility encrypts the data block with the received Data Key using AES-GCM block cipher for recording to media. A received DKx is automatically written to media using the Cartridge memory and the RW Head Interface. The decryption-on-the-fly check performs AES-GCM decryption of the encrypted data block and verifies the correctness of the encryption process	- Plaintext data - SEDK - DKx	- Encrypted data on tape - DKx on tape	User
Decrypting Read-type Command	- Host	The Secure Key Interface Facility automatically requests a key, provides authentication data and DKx information if available, securely transfers and verifies the key material. The received Data Key is used by the Data Block Cipher Facility to decrypt the data block with using AES-GCM decryption and returning plaintext data blocks to the host; Optionally in Raw mode the encrypted data block may be returned to the host in encrypted form (not supported in approved configuration)	SEDK	- Plaintext data to host	User
Set Encryption Control Parameters (including Bypass Mode)	- Host - Library	Performed via Mode Select to Mode Page x'25' and Encryption Subpage X'C0'	Requested Mode Page and Subpage	None	User
Query Encryption Control Parameters (including Bypass Mode)	- Host - Library	Performed via Mode Sense to Mode Page x'25' and Encryption Subpage X'C0'	Requested Mode Page and Subpage	Mode Data	User

Service	Interface(s)	Description	Inputs	Outputs	Role
Show Status (Visual Indicators)	- Front Panel LEDs and Single-Character Display	Visual indicators that an encryption operation is currently in progress may be monitored on the front panel	From LTO Gen5 drive operating system	Visual indicators on front panel	User
Drive Challenge/Response	- Host - Library	Allows programming challenge data and reading an optionally) encrypted, signed response; not used in default configuration. Performed via mode select and mode sense to Mode Page x'25' and Encryption Subpage x'D5'; not used in default configuration	Requested Mode Page and Subpage	Mode Data	User
Query Drive Certificate	- Host - Library	Allows reading of the Drive Certificate public key. Performed via mode sense to Mode Page x'25' and Encryption Subpage x'D6'; the provided certificate is signed by the IBM Tape Root CA.	Requested Mode Page and Subpage	Mode Data	User
Query dSK	- Host - Library	Allows reading of the Drive Session (Public) Key Performed via mode sense to Mode Page x'25' and Encryption Subpage X'DF' .	Requested Mode Page and Subpage	Mode Data	User
Setup SEDK structure (a protected key structure)	- Host - Library	This is the means to import a protected private key to the LTO Gen5 drive for use in writing and encrypted tape or in order to read a previously encrypted tape. Performed via mode select to Mode Page x'25' and Encryption Subpage x'E0'. In this service, the module generates a drive session key pair. The module then sends the dSK to the key manager where it is used to create an SEDK. Then, the key manager sends the SEDK back to the module.	Requested Mode Page and Subpage	Mode Data	User

Service	Interface(s)	Description	Inputs	Outputs	Role
Query DKx(s) – active, needed, pending , entire (all)	- Host - Library	Allows the reading from the drive of DKx structures in different categories for the medium currently mounted. Performed by Mode Select commands to Mode Page x25' and various subpages.	Requested Mode Page and Subpage	Mode Data	User
Request DKx(s) Translate	- Host - Library	This status command is used when the drive has already notified the Key Manager that is has read DKx structures from a mounted, encrypted tape and needs them translated to an SEDK and returned for the drive to read the tape. The key manager issues this command to read DKx structures which the drive requires to be translated by the Key Manager and subsequently returned to the drive as an SEDK structure to enable reading of the currently active encrypted area of tape. Performed via mode sense to Mode Page x'25' and Encryption Subpage X'EE'.	Requested Mode Page and Subpage	Mode Data	User
Request DKx(s) Generate	- Host - Library	This status command is used when the drive has already notified the Key Manager that it requires new SEDK and DKx structures to process a request to write an encrypted tape. This page provides information about the type of key the drive is requesting. Performed via mode sense to Mode Page x'25' and Encryption Subpage X'EF'.	Requested Mode Page and Subpage	Mode Data	User

Service	Interface(s)	Description	Inputs	Outputs	Role
Alter DKx(s)	- Host - Library	This command is used to modify the DKx structures stored to tape and cartridge memory. The LTO Gen5 drive will write the modified structures out to the tape and cartridge memory as directed. Performed via mode sense to Mode Page x'25' and Encryption Subpage x'E1'.	Requested Mode Page and Subpage	Mode Data	User
Drive Error Notify and Drive Error Notify Query	- Host - Library	These status responses are the means used by the drive to notify the Key Manager that an action is required, such as a Key generation or Translate, to proceed with an encrypted write or read operation. These status responses are read via Mode Sense commands to Mode Page x'25' subpage 'EF" and 'FF'.	Requested Mode Page and Subpage	Mode Data	User
Power-Up Self-Tests	- Power - Host - Library	Performs integrity and cryptographic algorithm self-tests, firmware image signature verification	None required	Failure status, if applicable	User, Crypto Officer
Configure Drive Vital Product Data (VPD) settings	- Host - Library	Allows controlling of default encryption mode and other operating parameters	From LTO Gen5 drive operating system	Vital Product Data (VPD)	User
Key Path Check diagnostic	- Host	As documented in the LTO Ultrium Tape Drive SCSI Reference	Send Diagnostic command specifying the Key Path diagnostic	Send Diagnositc command status	User
Key Zeroization	- Host	Zeroes all private plaintext keys in the LTO Gen5 drive via a Send Diagnostic command with Diagnostic ID EFFFh, as documented in the IBM TotalStorage LTO Ultrium Tape Drive SCSI Reference.	Send Diagnostic command specifying the Key Zeroization	Send Diagnositc command status	Crypto Officer
Firmware Load	- Host	Load new firmware to the module	New firmware	Load test indicator	Crypto Officer

3.5 Physical Security

The LTO Gen5 drive cryptographic boundary is the drive "brick" unit. The drive brick unit has industrial grade covers, and all the drive's components are production grade. The LTO Gen5 drive requires no preventative maintenance, and field repair is not performed for the unit. The drive brick covers are not removed in the field in the approved configuration. All failing units must be sent intact to the factory for repair.

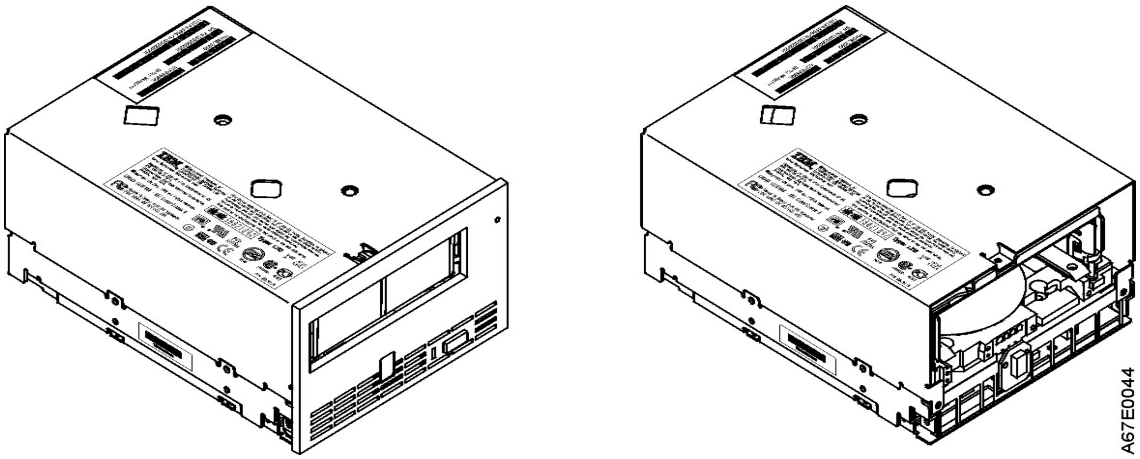


Figure 2 LTO Gen5 Drive Brick

3.6 Cryptographic Algorithms and Key Management

3.6.1 Cryptographic Algorithms

The LTO Gen5 drive supports the following basic cryptographic functions. These functions are used by the Secure Key Interface Facility or the Data Block Cipher Facility to provide higher level user services.

Table 6: Basic Cryptographic Functions

Algorithm	Type /Usage	Specification	Approved?	Used by	Algorithm Certificate
AES-ECB mode encryption/decryption (256-bit keys)	Symmetric cipher provides underlying AES for the AES Key Wrapping mechanism	AES: FIPS 197	Yes	Firmware	#1530
AES-GCM mode encryption / decryption (256-bit keys)	Symmetric Cipher Encrypts data blocks while performing decrypt-on-the-fly verification Decrypts data blocks	AES: FIPS-197 GCM: SP800-38D	Yes	ASIC	#1531 and #1532
RNG	IV generation for AES-GCM, Drive Session Key generation	FIPS-186-2 using SHA-1	Yes	Firmware	#825
SHA-1	Hashing Algorithm Multiple uses	FIPS-180-3	Yes	Firmware	#1361
SHA-256	Hashing Algorithm Digest checked on key manager messages, digest appended on messages to key manager	FIPS-180-3	Yes	Firmware	#1361
PKCS #1 :RSA Sign/Verify	Digital signature generation and verification to sign the session key and to verify firmware image signature on firmware load	FIPS 186-2 and PKCS#1	Yes	Firmware	#744
PKCS #1 :RSA Key Generation (1024/2048-bit keys)	Key Generation Session key generation	-	No, but allowed in FIPS mode[1]	Firmware	N/A
PKCS #1 RSA Key Transport (1024/2048-bit keys)	Decryption of transported key material SEDK	-	No, but allowed in FIPS mode	Firmware	N/A
TRNG (Custom)	Seeding RNG	-	No[2]	ASIC	N/A
AES Key Wrapping	Use served key to encrypt drive-generated data encrypting key	-	No, but allowed in FIPS mode	Firmware	Relies upon AES Cert. #1530

[1] Allowed for generation of keys used by the RSA Key Transport mechanism
[2] Allowed in FIPS mode for seeding approved RNG

3.6.2 Security Parameters

The following table provides a summary of both critical security parameters (CSPs) and non-critical security parameters used by the LTO Gen5 drive.

Table 7: Security Parameters

Security Parameter	CSP	Key Type	Input into Module	Output from Module	Generation Method	Storage Location	Storage Form	Zeroized
Drive Certificate Public Key (dCert)	No	RSA 2048-bit PKCS#1	Yes - at time of manufacture	Yes	N/A	Drive Vital Product Data (VPD)	Non-volatile Plaintext	N/A
Drive Certificate Private Key (dCert')	Yes	RSA 2048-bit PKCS#1	Yes - at time of manufacture	No	N/A	Drive VPD	Non-volatile X.509 certificate signed with the IBM Tape root CA	Yes
Drive Session Public Key (dSK)	No	RSA 2048-bit PKCS#1	No – Generated by module	Yes	Non-approved, allowed in FIPS mode	Drive RAM	Ephemeral Plaintext	N/A
Drive Session Private Key (dSK')	Yes	RSA 2048-bit PKCS#1	No – Generated by module	No	Non-approved, allowed in FIPS mode	Drive RAM	Ephemeral Plaintext	Yes
Data Key (DK)	Yes	AES 256-bit symmetric key	Yes – (Received in encrypted form)	No	N/A	Before Use: Drive RAM When in use: Stored In ASIC; (unreadable register)	Ephemeral Plaintext	Yes
Cryptographic Data Key (cDK)	Yes	AES 256-bit symmetric key	No – Generated by module	No	PRNG	Before Use: Drive RAM When in use: Stored in ASIC (unreadable register)	Ephemeral plaintext Ephemeral encrypted form as wDK	Yes
186-2 RNG Key	Yes	Seed	No – Generated by module	No	TRNG	Drive RAM	Ephemeral Plaintext	Yes
186-2 RNG Seed	Yes	Seed (20 bytes)	No – Generated by module	No	TRNG	Drive RAM	Ephemeral Plaintext	Yes

Additional notes on key management:

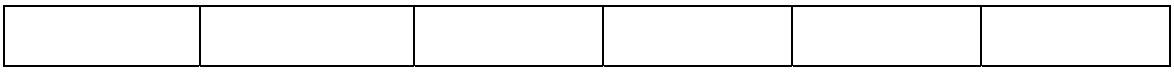
- Secret and private keys are never output from the LTO Gen5 drive in plaintext form.
- Secret keys may only be imported to the LTO Gen5 drive in encrypted form.

3.6.3 Self-Test

The LTO Gen5 drive performs both Power On Self Tests and Conditional Self tests as follows.
The operator shall power cycle the device to invoke the Power On Self tests.

Table 8: Self-Tests

Function Tested	**Self-Test Type**	**Implementation**
AES-ECB	Power-up	KAT performed for Encrypt and Decrypt
AES-GCM (256-bit keys)	Power-Up	KAT performed for Encrypt and Decrypt (256-bit)
RNG	Power-Up	KAT performed
SHA-1	Power-Up	KAT performed
SHA-256	Power-Up	KAT performed
RSA PKCS#1 Sign/Verify	Power-Up	KAT performed
Firmware Integrity Check	Power-Up	RSA PKCS #1 digital signature verification of application firmware; CRC check of SH vital product data (VPD); CRC check of FPGA image.
RNG	Conditional: When a random number is generated	Ensure the newly generated random number does not match the previously generated random number. Also ensure the first number generated after start up is not used and is stored for the next comparison
TRNG (Custom)	Conditional: When a random number is generated	Ensure the newly generated random number does not match the previously generated random number. Also ensure the first number generated after start up is not used and is stored for the next comparison
Firmware Load Check	Conditional: When new firmware is loaded or current firmware is re-booted	RSA PKCS #1 signature verification of new firmware image before new image may be loaded
Exclusive Crypto Bypass Test	Conditional: When switching between encryption and bypass modes	Ensure the correct output of data after switching modes Check to ensure the key is properly loaded



3.6.4 Bypass States

The LTO Gen5 drive supports a single static bypass mode. Bypass entry, exit, and status features are provided to meet approved methods for use of bypass states.

Two independent internal actions are required to activate bypass mode. First, the LTO Gen5 drive checks the host interface on which the bypass request was received for transmission errors. Then the LTO Gen5 drive checks the settings in the Encryption Control 1 field of Mode Page X'25' to determine if the bypass capability is enabled.

3.7 Design Assurance

LTO Gen5 drive release parts are maintained under the IBM Engineering Control (EC) system. All components are assigned a part number and EC level and may not be changed without re-release of a new part number or EC level.

The following table shows the certified configuration for each host interfaces of the LTO Gen5 encrypting tape drive:

Table 9: Certified Configurations

IBM LTO Generation 5 Encrypting Tape Drive	Hardware Part Number	Hardware EC Level	Firmware Image
Fibre Channel Interface	45E8192	M11221	pf100923e.A9Q5.FC.fips.ro
SAS Interface	45E8193	M11221	pf100923e.A9Q5.SAS.fips.ro

3.8 Mitigation of other attacks

The LTO Gen5 drive does not claim to mitigate other attacks.