IBM® Corporation LTO Generation 7 and Generation 8 Encrypting Tape Drive

Non-proprietary Security Policy

Version 2 Revision 00

Table of Contents

List of Tables

1 Document History

Date	Author	Change
2018/07/12	Kevin Butt	Initial conversion from LTO-7 Security Policy to LTO-8 Security Policy
2018/07/25	Kevin Butt	Updated Table 1: Certified Configurations
2018/08/24	Kevin Butt	Corrected omission of LTO-7 configurations in Table 14. Made changes to have the document talk to both LTO-7 and LTO-8
2018/10/04	Kevin Butt	Corrected part numbers in Table 14 in section 3.7 Design Assurance

2 Introduction

This non-proprietary security policy describes the IBM® Corporation LTO Generation 7 and Generation 8 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 IBM® Corporation LTO Generation 7 and Generation 8 Encrypting Tape Drive. The IBM® Corporation LTO Generation 7 and Generation 8 Encrypting Tape Drive is referred to in this document as the LTO Gen 7 and Gen 8, the IBM LTO Gen 7 and Gen 8, the Dell LTO Gen 7 and Gen 8, and the Oracle LTO Gen 7 and Gen 8.

The security policy document is organized in the following sections:

Introduction

- References
- Document Organization

LTO Gen 7 and Gen 8 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

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/

Table 2: Security Section

Security Section	Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services, and Authentication	1
Finite State Model	1
Physical Security	1
Operational Environment	NA
Cryptographic Key Management	1
EMI/EMC	1

Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	NA
Overall	1

2.1 References

This document describes only the cryptographic operations and capabilities of the LTO Gen 7 and Gen 8. More information is available on the general function of the LTO Gen 7 and Gen 8 at the IBM web site:

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

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

The LTO Gen 7 and Gen 8 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 IBM tape encryption and user configuration in various environments can be found at:

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

The LTO Gen 7 and Gen 8 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 LTO Gen 7 and Gen 8 Cryptographic Module Description

3.1 Overview

The LTO Gen 7 and Gen 8, also referred to herein as 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 Gen 7 and Gen 8 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. Some components of the LTO Gen 7 and Gen 8 tape drive, such as mechanical components used for tape loading/unloading and actuating the tape cartridge, labels, cables, connectors, terminals and sensor components, do not have an effect on the security of the cryptographic module.

Block diagrams of the LTO Gen 7 and Gen 8 are shown below:

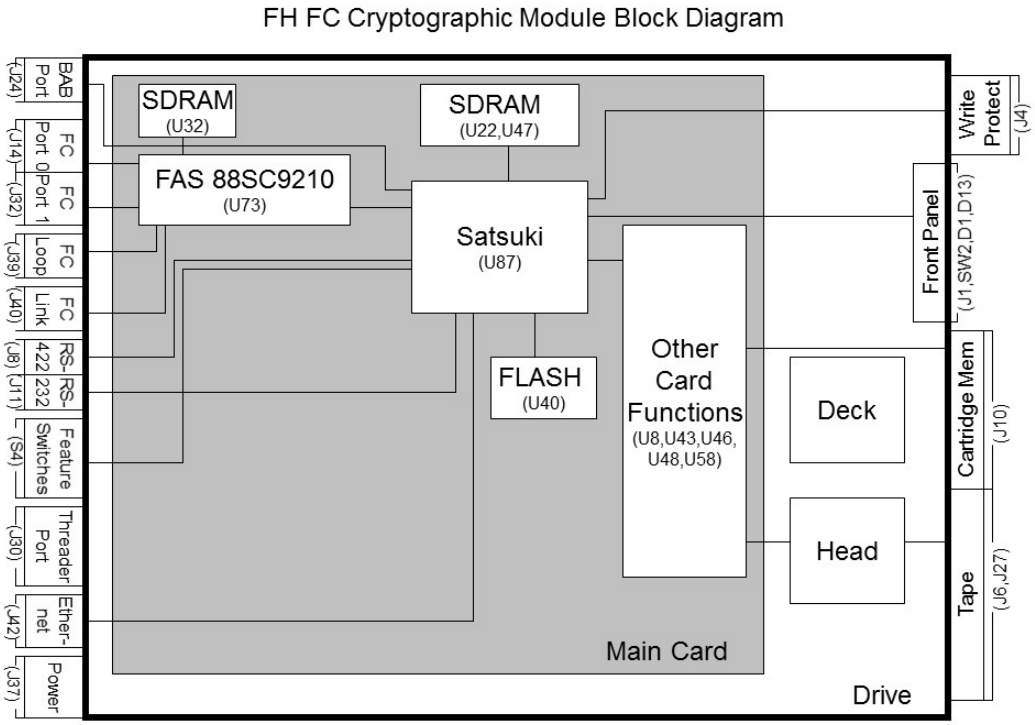

Figure 1a: LTO Gen 7 and Gen 8 Full-High Fibre Channel Drive Block Diagram

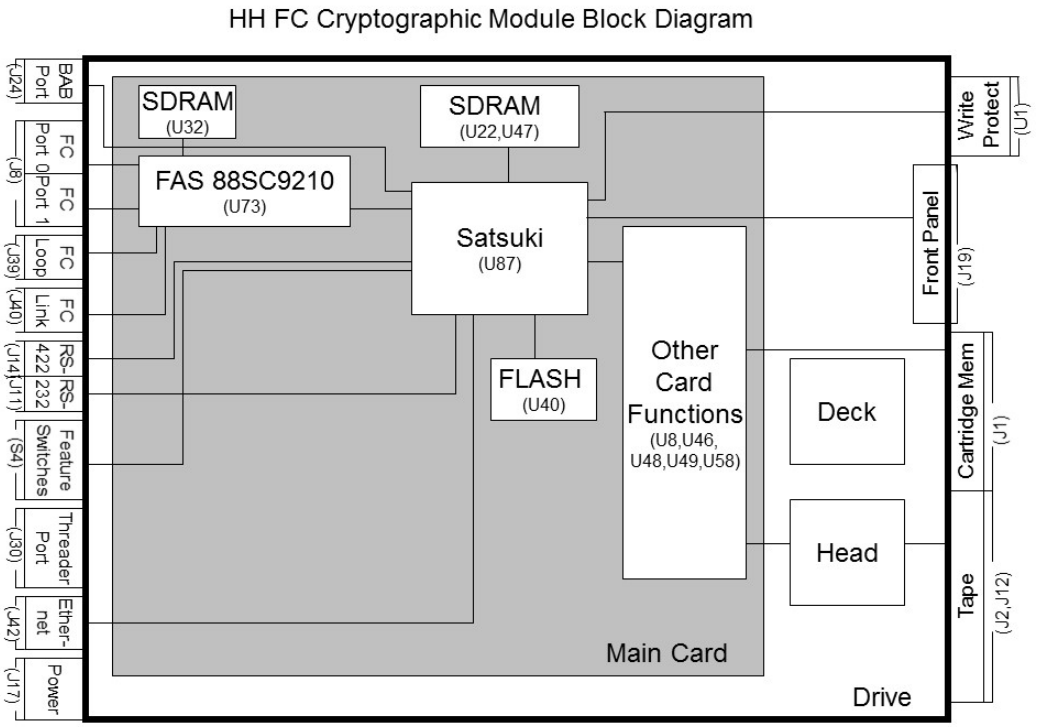

Figure 1b: LTO Gen 7 and Gen 8 Half-High Fibre Channel Drive Block Diagram

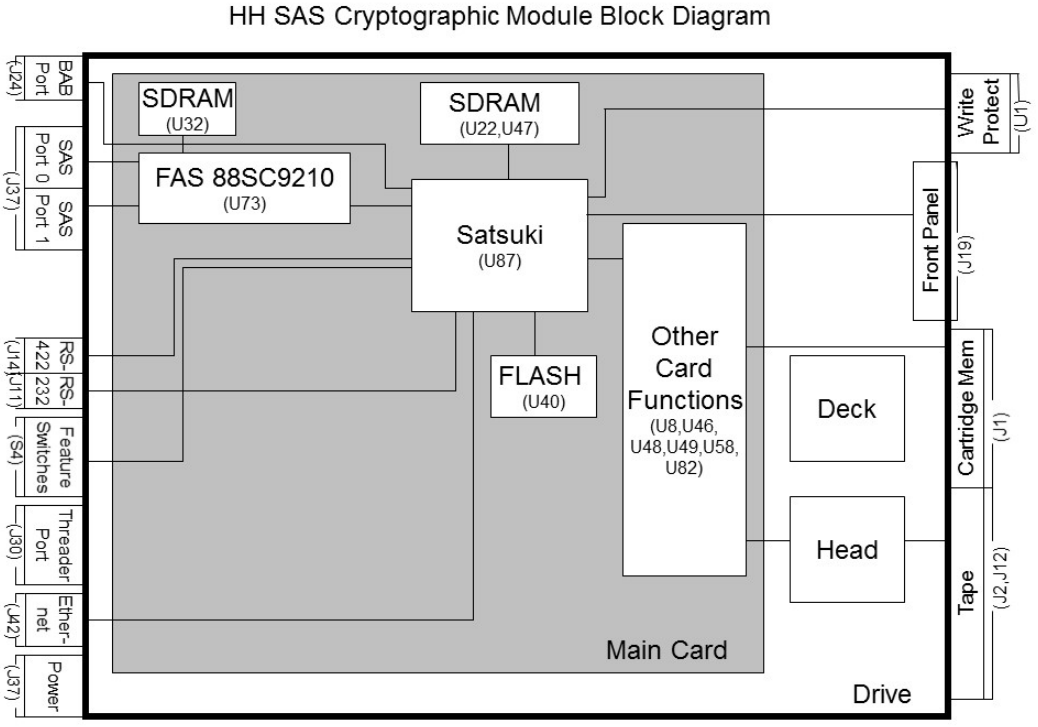

Figure 1c: LTO Gen 7 and Gen 8 Half-High SAS Drive Block Diagram

The LTO Gen 7 and Gen 8 has two major cryptographic functions:

- Data Block Cipher Facility: The tape drive has the ability to encrypt and decrypt standard tape data blocks as received via SCSI write- and read-type commands. Encryption and decryption is performed using a provided key and AES-GCM block cipher.
    - 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 Gen 7 and Gen 8 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: Tape drive functions allow authentication of the tape drive to an external IBM key manager, such as the IBM Encryption Key Manager (EKM), the Tivoli Key Lifecycle Manager (TKLM), or the IBM Security Key Lifecycle Manager (ISKLM), 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 Gen 7 and Gen 8 drive to maintain FIPS-140 validation.

There are three configurations for the LTO Gen 7 and Gen 8 in the approved mode of operation. They are:
- System-Managed Encryption (SME)
- Library-Managed Encryption (LME)
- T10 SCSI Encryption mode

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.

The LTO Gen 7 and Gen 8 is in the approved mode of operation when a SCSI Mode Sense command to Mode Page 25h returns the values in Table 2: Reported Values Indicating Approved Modes of Operation and an Allowed service from Table 3: Host Interface Mode Select Eligibility of Mode Page 30h, Subpage 20h and Mode Page 25h Subpages is used.

Table 3: Reported Values Indicating Approved Modes of Operation

Required Fields	**System-Managed Encryption (SME)**	**Library-Managed Encryption (LME)**	**T10 SCSI Encryption**	
			Via library interface	Via host interface
Key Path (Manager Type) (from VPD) Mode Page 25h, byte 21, bits 7-5	001b	110b	000b	101b
In-band Key Path (Manager Type) Override Mode Page 25h, byte 21, bits 4-2	000b or 001b	000b	000b	000b
Indirect Key Mode Default Mode Page 25h, byte 22, bit 4	0b	0b	0b	0b

Key Scope Mode Page 25h, byte 23, bits 2-0	000b or 001b	000b or 001b	000b	000b
Encryption Method Mode Page 25h, byte 27	10h or 1Fh	60h	60h	50h

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 and T10 SCSI encryption configurations, all Mode Select commands to Mode Page 30h, Subpage 20h and all subpages of Mode Page 25h are prohibited on the host interface. In the SME configuration, Mode Select commands to Mode Page 30h, Subpage 20h and the following subpages of Mode Page 25h are prohibited.

Table 4: Host Interface Mode Select Eligibility of Mode Page 30h, Subpage 20h and Mode Page 25h Subpages

Mode Page	Mode Subpage	System-Managed Encryption (SME)	Library-Managed Encryption (LME)	T10 SCSI Encryption
25h	C0h – Control/Status	**Allowed**	Prohibited	Prohibited
25h	D0h – Generate dAK/dAK' Pair	Prohibited	Prohibited	Prohibited
25h	D1h – Query dAK	Prohibited	Prohibited	Prohibited
25h	D2h – Update dAK/dAK' Pair	Prohibited	Prohibited	Prohibited
25h	D3h – Remove dAK/dAK' Pair	Prohibited	Prohibited	Prohibited
25h	D5h – Drive Challenge/Response	Prohibited	Prohibited	Prohibited
25h	D6h – Query Drive Certificate	**Allowed**	Prohibited	Prohibited
25h	D7h – Query/Setup HMAC[1]	Prohibited	Prohibited	Prohibited
25h	D8h – Install eAK	Prohibited	Prohibited	Prohibited
25h	D9h – Query eAK	Prohibited	Prohibited	Prohibited
25h	DAh – Update eAK	Prohibited	Prohibited	Prohibited
25h	DBh – Remove eAK	Prohibited	Prohibited	Prohibited
25h	DFh – Query dSK	**Allowed**	Prohibited	Prohibited
25h	E0h – Setup SEDK	**Allowed**	Prohibited	Prohibited
25h	E1h – Alter DKx	Prohibited	Prohibited	Prohibited
25h	E2h – Query DKx (Active)	**Allowed**	Prohibited	Prohibited
25h	E3h – Query DKx (Needed)	**Allowed**	Prohibited	Prohibited
25h	E4h – Query DKx (Entire)	**Allowed**	Prohibited	Prohibited
25h	E5h – Query DKx (Pending)	**Allowed**	Prohibited	Prohibited
25h	EEh – Request DKx (Translate)	Prohibited	Prohibited	Prohibited
25h	EFh – Request DKx (Generate)	**Allowed**	Prohibited	Prohibited
25h	FEh – Drive Error Notify	**Allowed**	Prohibited	Prohibited
30h	20h – Encryption Mode	Prohibited	Prohibited	Prohibited

Key:
Allowed –Use of this function in this encryption mode is considered to be operating in an approved mode.
Prohibited – Use of this function in this encryption mode is considered to be operating in a non-approved mode.

[1] This is a misnomer in that this is a message signature setup function. No HMAC is supported. This is a SHA 2 256 digest used for message integrity only.

Loading a FIPS 140-2 validated drive microcode level and configuring the drive for one of the approved modes of operation initializes the LTO Gen 7 and Gen 8 into the approved mode of operation. The FIPS 140-2 validated drive microcode level should be loaded twice to ensure the firmware occupies both the main and reserved firmware locations.

The LTO Gen 7 and Gen 8 supports multi-initiator environments, but only one initiator may access cryptographic functions at any given time. Therefore the LTO Gen 7 and Gen 8 does not support multiple concurrent operators.

The LTO Gen 7 and Gen 8 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 Gen 7 and Gen 8 drive operates as a stand-alone tape drive and has no direct dependency on any specific operating system or platform for FIPS approved operating modes, 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 the SME and LME modes of operation, a key manager, such as the Encryption Key Manager (EKM), the Tivoli Key Lifecycle Manager (TKLM), or the IBM Security Key Lifecycle Manager (ISKLM), and a supported key store must be used in a manner which supports secure import and export of keys with the LTO Gen 7 and Gen 8 drive :
    - Keys must be securely passed into the LTO Gen 7 and Gen 8 drive.
      - For SME and LME, the key manager must support encryption of the Data Key to form an Session Encrypted Data Key (SEDK) for transfer to the LTO Gen 7 and Gen 8 drive using the LTO Gen 7 and Gen 8 drive public Session Key and a 2048-bit RSA encryption method.
      - For T10 SCSI encryption, the host must support RSA key wrapping.
    - 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 Gen 7 and Gen 8 drive must be configured in one of the approved modes of operation.
  - The LTO Gen 7 and Gen 8 drive must have the FIPS 140-2 validated drive firmware level loaded and operational.
  - In LME mode, the LTO Gen 7 and Gen 8 drive must be operated in an automation device which conforms to the LDI or ADI interface specifications provided.
  - In T10 SCSI encryption mode via the library interface, the LTO Gen 7 and Gen 8 drive must be operated in an automation device which conforms to the ADI interface specifications provided.

3.3 Ports and Interfaces

The cryptographic boundary of the LTO Gen 7 and Gen 8 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 operations) 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 5: Ports Common to All Host Interface Types

LTO Gen 7 and Gen 8 Drive Physical Ports	**FIPS-140-2 Logical Interface**	**Crypto Services**	**Interface Functionality**
BAB Port	Status Output	None	▪ Outputs servo status
RS-422 Port / sADT Port or LDI Port	Data Input Data Output Control Input Status Output	Yes	▪ Crypto: Inputs protected keys from the key manager in some LME mode configurations and T10 SCSI encryption mode. ▪ Inputs data ▪ Outputs data ▪ Outputs status ▪ Outputs encrypted key components ▪ Inputs LDI and ADI protocol commands. ▪ Outputs LDI and ADI protocol status. ▪ Inputs ADC SCSI commands. ▪ Outputs ADC SCSI status.
RS-232 Port	Disabled	None	▪ Disabled by FIPS approved firmware levels.
Ethernet Port / iADT port	Data Input Data Output Control Input Status Output	Yes	▪ Inputs controls and image for firmware load ▪ Crypto: Inputs protected keys from the key manager in some LME mode configurations and T10 SCSI encryption mode. ▪ Inputs data ▪ Outputs data ▪ Outputs status ▪ Outputs encrypted key components ▪ Inputs ADI protocol commands. ▪ Outputs ADI protocol status. ▪ Inputs ADC SCSI commands. ▪ Outputs ADC SCSI 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 Gen 7 and Gen 8 drive
Write Protect Switch (FH models only)	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

LTO Gen 7 and Gen 8 Drive Physical Ports	**FIPS-140-2 Logical Interface**	**Crypto Services**	**Interface Functionality**
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 encrypted data indicator ▪ Outputs parameters. ▪ Crypto: Outputs encrypted data indicator
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 6: Fibre Channel-Specific Host Interfaces Ports

LTO Gen 7 and Gen 8 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 and T10 SCSI encryption mode via the host interface. ▪ Outputs data ▪ Outputs encrypted key components ▪ Inputs SCSI commands ▪ Outputs SCSI 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 7: SAS-Specific Host Interfaces Ports

LTO Gen 7 and Gen 8 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 SCSI commands ▪ Outputs SCSI 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 Gen 7 and Gen 8 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 Gen 7 and Gen 8 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 Gen 7 and Gen 8 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 Gen 7 and Gen 8 drive. Under these circumstances the LTO Gen 7 and Gen 8 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 Gen 7 and Gen 8 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. All of the service summarized here, excluding the services expressly prohibited in Table 3, are allowed in the FIPS mode of operation.

Table 8: Provided Services Applicable to All Modes of Operation

Service	Interface(s)	Description	Inputs	Outputs	Role
General SCSI commands	- Host	As documented in the IBM TotalStorage LTO Ultrium Tape Drive SCSI Reference	See description	See description	User
General Library Interface commands	- Library	As documented in the IBM Library/Drive Interface Specification and IBM ADI Implementation Reference	See description	See description	User
Load tape	- Host/Library - Manual insertion	Load tape can be performed by an operator manually inserting a tape cartridge into the drive throat or via commands over the host or library interface	See description	Green LED flashes while the load is in progress	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 interface	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
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 Gen 7 and Gen 8 drive operating system	Visual indicators on front panel	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 Gen 7 and Gen 8 drive operating system	Vital Product Data (VPD)	User
Key Path Check diagnostic	- Host	As documented in the IBM TotalStorage LTO Ultrium Tape Drive SCSI Reference	Send Diagnostic command specifying the Key Path diagnostic	Send Diagnostic command status	User
Key Zeroization	- Host	Zeroes all private plaintext keys in the LTO Gen 7 and Gen 8 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 Diagnostic command status	Crypto Officer
Firmware Load	- Host	Load new firmware to the module	New firmware	Load test indicator	Crypto Officer

Table 9: Provided Services Applicable to SME and LME

Service	Interface(s)	Description	Inputs	Outputs	Role
Encrypting Write-type Command	- Host	The Secure Key Interface Facility automatically requests a DK and DKx, if needed. The Data Block Cipher Facility encrypts the data block with the cDK using AES-GCM block cipher for recording to media. A DKx and wDK is automatically written to media using 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	- Encrypted data on tape - DKx on tape - wDK on tape	User
Decrypting Read-type Command	- Host	The Secure Key Interface Facility automatically requests a DK, if needed. The cDK 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)		- Plaintext data to host	User
Set Encryption Control Parameters (including Bypass Mode)	- Host - Library	Performed via Mode Select to Mode Page 25h and Encryption Subpage C0h	Requested Mode Page and Subpage	None	User
Query Encryption Control Parameters (including Bypass Mode)	- Host - Library	Performed via Mode Sense to Mode Page 25h and Encryption Subpage C0h	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 25h and Encryption Subpage D6h; 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 25h and Encryption Subpage DFh.	Requested Mode Page and Subpage	Mode Data	User

Service	Interface(s)	Description	Inputs	Outputs	Role
Setup SEDK structure (a protected key structure)	- Host - Library	This is the means to import a protected private key to the LTO Gen 7 and Gen 8 drive for use in writing and encrypted tape or in order to read a previously encrypted tape. Performed via mode select to Mode Page 25h and Encryption Subpage E0h. 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.	SEDK and DKx	Status (none)	User
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 25h and various subpages.	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 25h and Encryption Subpage EFh.	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 25h subpage EFh and FFh.	Requested Mode Page and Subpage	Mode Data	User

Table 10: Provided Services Applicable to T10 SCSI Encryption

Service	Interface(s)	Description	Inputs	Outputs	Role

Service	Interface(s)	Description	Inputs	Outputs	Role
Encrypting Write-type command	- Host	The Secure Key Interface Facility requests a DK, if needed. The Data Block Cipher Facility encrypts the data block with the cDK using AES-GCM block cipher for recording to media. A DKx and wDK is automatically written to media using 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	- Encrypted data on tape - DKx on tape - wDK on tape	User
Decrypting Read-type Command	- Host - Library	The Secure Key Interface Facility requests a DK, if needed. The cDK is used by the Data Block Cipher Facility to decrypt the data block 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)		- Plaintext data to host	User
Query Data Encryption Status: SPIn (20h[0020h])	- Host - Library	Performed via Security Protocol In[2] Security Protocol 20h, Security Protocol Specific 0020h.	Requested security protocol specific	DKx Bypass Mode settings	User
Query Next Block Encryption Status: SPIn (20h[0021h])	- Host - Library	Performed via Security Protocol In Security Protocol 20h, Security Protocol Specific 0021h.	Requested security protocol specific	DKx	User
Query Device Server Key Wrapping Public Key: SPIn (20h[0031h])	- Host - Library	Performed via Security Protocol In Security Protocol 20h, Security Protocol Specific 0031h.	Requested security protocol specific	Public key for RSA-wrapping	User
Report Data Encryption Policy SPIn (21h[0010h])	- Host - Library	Performed via Security Protocol In Security Protocol 21h, Security Protocol Specific 0010h.	Requested security protocol specific	Control Policy Code	User

[2] For more information on the Security Protocol In command see ISO/IEC 14776-334, SCSI Stream Commands - 4 (SSC-4) and for the specific implementation in this device see IBM® TotalStorage® LTO Ultrium Tape Drive SCSI Reference (GA32-0928-03).

Service	Interface(s)	Description	Inputs	Outputs	Role
Set Data Encryption: SPOut (20h[0010h])	- Host - Library	Performed via Security Protocol Out[3] Security Protocol 20h, Security Protocol Specific 0010h.	Security protocol parameters, optionally RSA-wrapped data key, DKx	None	User
Select Data Encryption Parameters Complete: SPOut (20h[0030h])	- Library	Performed via Security Protocol Out Security Protocol 20h, Security Protocol Specific 0030h.	Security protocol parameters	None	User
Configure Encryption Policy: SPOut (21h[0011h])	- Library	Performed via Security Protocol Out Security Protocol 21h, Security Protocol Specific 0011h. Configure Encryption Policy	Security protocol parameters	None	User

[3] For more information on the Security Protocol Out command see ISO/IEC 14776-334, SCSI Stream Commands - 4 (SSC-4) and for the specific implementation in this device see IBM® TotalStorage® LTO Ultrium Tape Drive SCSI Reference (GA32-0928-03).

3.5 Physical Security

The LTO Gen 7 and Gen 8 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 Gen 7 and Gen 8 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.

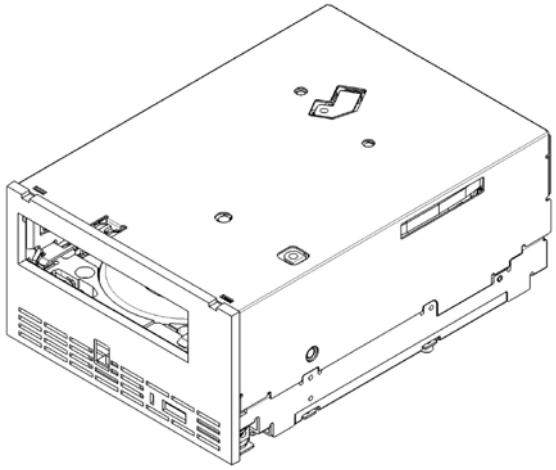

Figure 2a: Front View of LTO Gen 7 and Gen 8 Full-High Fibre Channel Drive Brick

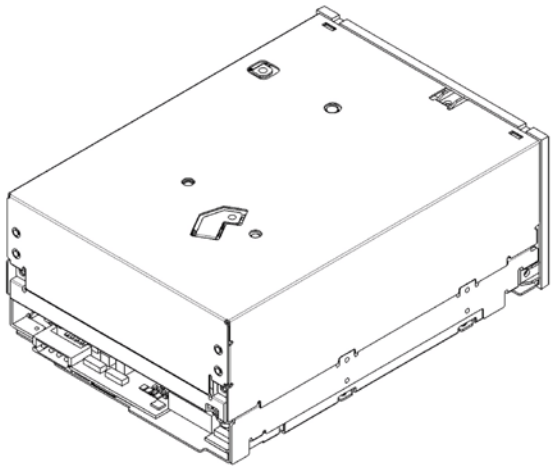

Figure 2b: Rear View of LTO Gen 7 and Gen 8 Full-High Fibre Channel Drive Brick

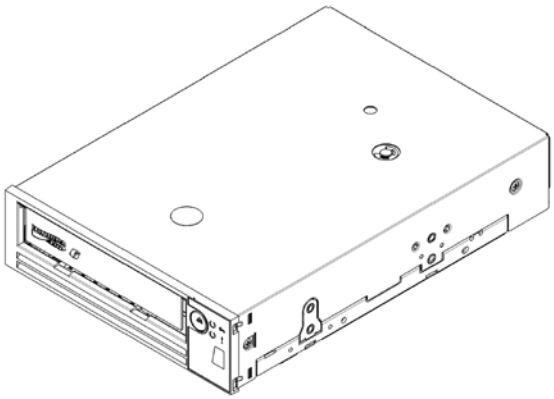

Figure 2c: Front View of LTO Gen 7 and Gen 8 Half-High Drive Brick

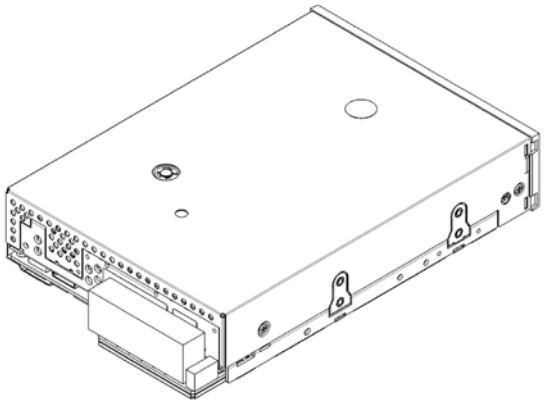

Figure 2d: Rear View of LTO Gen 7 and Gen 8 Half-High Fibre Channel Drive Brick

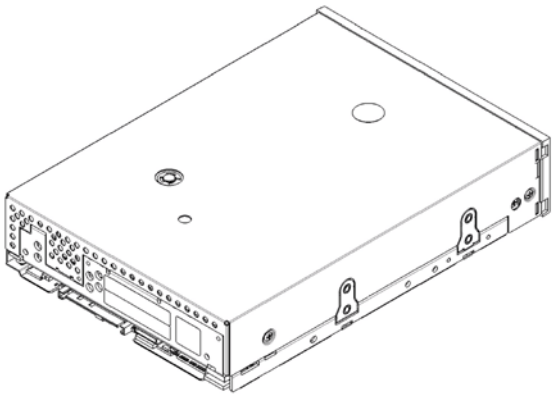

Figure 2e: Rear View of LTO Gen 7 and Gen 8 Half-High SAS Drive Brick

3.6 Cryptographic Algorithms and Key Management

3.6.1 Cryptographic Algorithms

The LTO Gen 7 and Gen 8 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. Note that algorithms in this table are subject to the transition tables from NIST SP 800-131A, which should be used to inform users of the risks associated with using a particular algorithm and a given key length.

Table 11: 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 encryption	AES: FIPS 197	Yes	Firmware	4810
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	3357 3358
DRBG	IV generation[4] for AES-GCM, Drive Session Key generation	SP800-90A using SHA-512	Yes	Firmware	1672
SHA-1	Hashing algorithm. Multiple uses	FIPS-180-4	Yes	Firmware	3954
SHA-256	Hashing algorithm digest checked on key manager messages, digest appended on messages to key manager	FIPS-180-4	Yes	Firmware	3954
SHA-512	Hashing algorithm supports DRBG	FIPS 180-4	Yes	Firmware	3954
RSA Sign/Verify	Digital signature using PKCS#1 with SHA256 hash and a 2048 bit key generation and verification to sign the dSK (session key) and to verify firmware image signature on firmware load	FIPS 186-4	Yes	Firmware	2634
RSA Key Generation (2048-bit keys)	Key Generation Session key generation	-	Yes	Firmware	N/A

[4] The IV is generated as 96 bits of random data by the DRBG and then incremented with each new use.

Algorithm	Type /Usage	Specification	Approved?	Used by	Algorithm Certificate
RSA Key Transport (2048-bit keys)	Decryption of transported SEDK key material + T10 Logical Block Encryption Key Format 02, Key wrapped by device server public key (provides 112 bits of encryption strength)	-	No, but allowed in FIPS mode	Firmware	N/A
NDRNG (TRNG) (Custom)	Seeding DRBG	-	No, but allowed in FIPS mode[5]	ASIC	N/A
AES Key Wrapping (256-bit keys)	Symmetric Cipher Wraps/Unwraps the cDK	SP800-38F	Yes	Firmware	4810

[5] Allowed in FIPS mode for seeding approved DRBG

3.6.2 Security Parameters

This table lists LTO Gen 7 and Gen 8 drive critical security parameters (CSPs) and non-critical security parameters.

Table 12: Security Parameters

Security Parameter	CSP	Key Type	Input into Module	Output from Module	Generation Method[6]	Storage Location	Storage Form	Zeroized
Drive Certificate Public Key (dCert)	No	RSA 2048-bit	Yes - at time of manufacture	Yes, in X.509 format	N/A	Drive Vital Product Data (VPD)	Non-volatile Plaintext	N/A
Drive Certificate Private Key (dCert')	Yes	RSA 2048-bit	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	No – Generated by module	Yes, in plaintext	FIPS 186-4	Drive RAM	Ephemeral Plaintext	N/A
Drive Session Private Key (dSK')	Yes	RSA 2048-bit	No – Generated by module	No	FIPS 186-4	Drive RAM	Ephemeral Plaintext	Yes
Data Key (DK)	Yes	AES 256-bit symmetric key	Yes – (Received encrypted by RSA 2048)	No	N/A	Drive RAM	Ephemeral Plaintext	Yes
Cryptographic Data Key (cDK)	Yes	AES 256-bit symmetric key	No – Generated by module	Yes, in AES Key Wrapped format	DRBG	Drive RAM	Ephemeral encrypted form as wDK	Yes
						When in use: Stored in ASIC (unreadable register)	Ephemeral encrypted form as wDK	
						Tape medium	Encrypted form as wDK	
DRBG Entropy Input String	Yes	256-bit input string	No – Generated by module	No	NDRNG (TRNG)	Drive RAM	Ephemeral Plaintext	Yes
DRBG value, V	Yes	256 bits	No – Generated by module	No	Internal state value of DRBG	Drive RAM	Ephemeral Plaintext	Yes
DRBG constant, C	Yes	256 bits	No – Generated by module	No	Internal state value of DRBG	Drive RAM	Ephemeral Plaintext	Yes

[6] For all keys denoted as being generated by the module, the symmetric keys are produced using the unmodified output of the DRBG, and the seeds used in asymmetric key generation are produced using the unmodified output of the DRBG

Security Parameter	**CSP**	**Key Type**	**Input into Module**	**Output from Module**	**Generation Method[6]**	**Storage Location**	**Storage Form**	**Zeroized**
RSA public key (used for firmware image verification)	No	RSA 2048-bit	Yes - In firmware image	No	N/A	Drive RAM, FLASH, Firmware Image	Non-volatile Plaintext	N/A

Additional notes on key management:

- Secret and private keys are never output from the LTO Gen 7 and Gen 8 drive in plaintext form.
- Secret keys may only be imported to the LTO Gen 7 and Gen 8 drive in encrypted form.
- Zeroization behavior outlines in Table 12.

Table 13: CSP Access Table

	Drive Certificate Public Key (dCert)	Drive Certificate Private Key (dCert')	Drive Session Public Key (dSK)	Drive Session Private Key (dSK')	Data Key (DK)	Cryptographic Data Key	DRBG Entropy Input Key	DRBG value ,V	DRBG Constant, C	RSA public key for firmware image verification
General SCSI commands										
General Library Interface commands	R		R							
Service Panel Configuration										
Service Panel Diagnostics					X	X	X	X	X	
Service Panel Status Display										
Front Panel Interface Status										
Front Panel Interface Unload			W	W	W	W				
Front Panel Interface Reset			W	W	W	W	W	W	W	
Encrypting Write-type Command					X	X				
Decrypting Read-type Command					X	X				
Set Encryption Control Parameters (including Bypass Mode)										
Query Encryption Control Parameters (including Bypass Mode)										
Query Drive Certificate	R									
Query dSK		X	R							
Setup an SEDK structure (a protected key structure)				X	W					
Drive Error Notify and Drive Error Notify Query										
Security Protocol In, Device Server Key Wrapping Public Key page			R							
Security Protocol Out, Set Data Encryption page				X	W					
Power-Up Self-Tests					X	X	X	X	X	
Configure Drive Vital Product Data (VPD) settings	W	W								
Key Path Check diagnostic	X	X	RX	X						
Key Zeroization	W	W	W	W	W	W	W	W	W	

	Drive Certificate Public Key (dCert)	Drive Certificate Private Key (dCert')	Drive Session Public Key (dSK)	Drive Session Private Key (dSK')	Data Key (DK)	Cryptographic Data Key	DRBG Entropy Input Key	DRBG value , V	DRBG Constant, C	RSA public key for firmware image verification
Firmware Load Test										X
Load tape							W			
Unload tape					W	W				
Enter manual diagnostic mode										
Scrolls through manual diagnostic functions										
Exits manual diagnostic mode										
Forces drive dump										
Resets the drive			W	W	W	W				
Show Status (Visual Indicators)										
Query DKx(s) – active, needed, pending, entire (all)										
Request DKx(s) Generate										
Query Data Encryption Status: SPIn (20h[0020h])										
Query Next Block Encryption Status: SPIn (20h[0021h])										
Query Device Server Key Wrapping Public Key: SPIn (20h[0031h])			R							
Report Data Encryption Policy SPIn (21h[0010h])										
Set Data Encryption: SPOut (20h[0010h])					W					
Select Data Encryption Parameters Complete: SPOut (20h[0030h])										
Configure Encryption Policy: SPOut (21h[0011h])										
Key: R – Read Access W – Write Access X – Execute Access										

3.6.3 Self-Test

The LTO Gen 7 and Gen 8 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 14: Self-Tests

Function Tested	**Self-Test Type**	**Implementation**	**Failure Behavior**
AES-ECB	Power-up	KAT performed for Encrypt and Decrypt	FSC 0x1130 posted
AES-GCM (256-bit keys)	Power-Up	KAT performed for Encrypt and Decrypt (256-bit)	FSC 0x1130 posted

Function Tested	Self-Test Type	Implementation	Failure Behavior
DRBG	Power-Up	KAT performed	FSC 0x1133 posted
SHA-1	Power-Up	KAT performed	FSC 0x1131 posted
SHA-256	Power-Up	KAT performed	FSC 0x1131 posted
SHA-512	Power-Up	KAT performed	FSC 0x1131 posted
RSA Sign KAT and Verify KAT	Power-Up	KAT performed	FSC 0x1131 posted
Firmware Integrity Check	Power-Up	RSA digital signature verification of application firmware; CRC check of SH vital product data (VPD); CRC check of FPGA image.	Drive reboot
VPD Integrity Check	Power-Up	CRC check of vital product data (VPD)	FSC 0x112E posted
DRBG	Conditional: When a random number is generated	Continuous random number generator test performed.	FSC 0x1133 posted
DRBG	Conditional: When random numbers are generated	SP800-90A DRBG Health Tests (Instantiate, Generate and Reseed)	FSC 0x1133 posted
NDRNG (TRNG) (Custom)	Conditional: When a random number is generated	Continuous random number generator test performed.	Drive reboot
RSA Pair-Wise Consistency	Conditional: When a new RSA key is generated	RSA Pair-Wise Consistency (Sign and Verify)	FSC 0x1133 posted
Firmware Load Check	Conditional: When new firmware is loaded or current firmware is re-booted	RSA signature verification of new firmware image before new image may be loaded	Drive rejects code load with FSC 0x5902
Exclusive 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.	Drive reboots and rejects failure injection code level.

3.6.4 Bypass States

The LTO Gen 7 and Gen 8 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 Gen 7 and Gen 8 drive checks the interface on which the bypass request was received for transmission errors. Then the LTO Gen 7 and Gen 8 drive checks the value of the received bypass instruction. For SME and LME the Encryption State field within the Encryption Control 1 field of Mode Page 25h to determines if the bypass capability is enabled. For T10 SCSI Encryption, the Encryption Mode and Decryption Mode fields of Security Protocol Out Security Protocol 20h, Security Protocol Specific 0010h.

3.7 Design Assurance

LTO Gen 7 and Gen 8 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 Gen 7 and Gen 8:

Table 15: Certified Configurations

Product	Hardware Part Number Hardware EC Level	Firmware Part Number Firmware EC Level	Firmware Image
IBM LTO Gen 7 FH FC	38L7450 M13681	38L7082 01PL103	LTO7_G986.fcp_fh_f.fmrz
IBM LTO Gen 7 HH FC	38L7464 M13681	38L7458 01PL105	LTO7_G986.fcp_hh_f.fmrz
IBM LTO Gen 7 HH SAS	38L7462 M13681	38L7095 01PL106	LTO7_G986.sas_hh_f.fmrz
Dell LTO Gen 7 FH FC	38L7450 M13681	38L7448 01PL104	LTO7_G986.fcp_fh_f_OEMD.fmrz
Dell LTO Gen 7 HH FC	38L7464 M13681	38L7654 01PL107	LTO7_G986.fcp_hh_f_OEMD.fmrz
Dell LTO Gen 7 HH SAS	38L7462 M13681	38L7651 01PL108	LTO7_G986.sas_hh_f_OEMD.fmrz
IBM LTO Gen 8 FH FC	01PL347 N99440	02PY098 M14321	LTO8_J4D0.fcp_fh_f.fmrz
IBM LTO Gen 8 HH FC	01PL351 N99440	02PY099 M14321	LTO8_J4D1.fcp_hh_f.fmrz
IBM LTO Gen 8 HH SAS	01PL349 N99440	02PY100 M14321	LTO8_J4D1.sas_hh_f.fmrz
Dell LTO Gen 8 FH FC	01PL347 N99440	02PY104 M14321	LTO8_J4D0.fcp_fh_f_OEMD.fmrz
Dell LTO Gen 8 HH FC	01PL351 N99440	02PY111 M14321	LTO8_J4D1.fcp_hh_f_OEMD.fmrz
Dell LTO Gen 8 HH SAS	01PL349 N99440	02PY115 M14321	LTO8_J4D1.sas_hh_f_OEMD.fmrz
Oracle LTO Gen 8 FH FC	01PL347 N99440	02PY122 M14321	LTO8_J4D0.fcp_fh_f_OEMS.fmrz
Oracle LTO Gen 8 HH FC	01PL351 N99440	02PY123 M14321	LTO8_J4D1.fcp_hh_f_OEMS.fmrz

Oracle LTO Gen 8 HH SAS	01PL349	02PY124	LTO8_J4D1.sas_hh_f_OEMS.fmrz
	N99440	M14321	

3.8 Mitigation of other attacks

The LTO Gen 7 and Gen 8 drive does not claim to mitigate other attacks.