Hewlett Packard
Enterprise

HPE LTO-7 and LTO-8 Encrypting Tape Drive

Non-proprietary Security Policy

Version: 2.0

Hewlett Packard
Enterprise

Table of Contents

List of Tables

Hewlett Packard
Enterprise

1 Document History

Date	Author	Version	Change
2018/06/25	Chris Martin	1.0	First version (LTO-7 only)
2019/03/08	Chris Martin	2.0	Add LTO-8

2 Introduction

This non-proprietary security policy describes the Hewlett Packard Enterprise 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 Hewlett Packard Enterprise LTO Generation 7 and Generation 8 Encrypting Tape Drive. The Hewlett Packard Enterprise LTO Generation 7 and Generation 8 Encrypting Tape Drive is referred to in this document as the HPE LTO-7 drive and the LTO-7 tape drive, and the HPE LTO-8 drive and the LTO-8 tape drive.

The security policy document is organized in the following sections:

Introduction

- References
- Document Organization

LTO-7 and LTO-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 1: 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 HPE LTO-7 and LTO-8 tape drives. More information on the general function of the LTO-7 and LTO-8 tape drives is available at the HPE web site:

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

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

The LTO-7 and LTO-8 tape drives support two 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/

The LTO-7 and LTO-8 tape 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 HPE and is releasable only under appropriate non-disclosure agreements. For access to these documents, contact HPE.

3 LTO-7 and LTO-8 Cryptographic Module Description

3.1 Overview

The HPE LTO-7 and LTO-8 tape drives, 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-7 or LTO-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-7 and LTO-8 tape drives, 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-7 and LTO-8 are shown below:

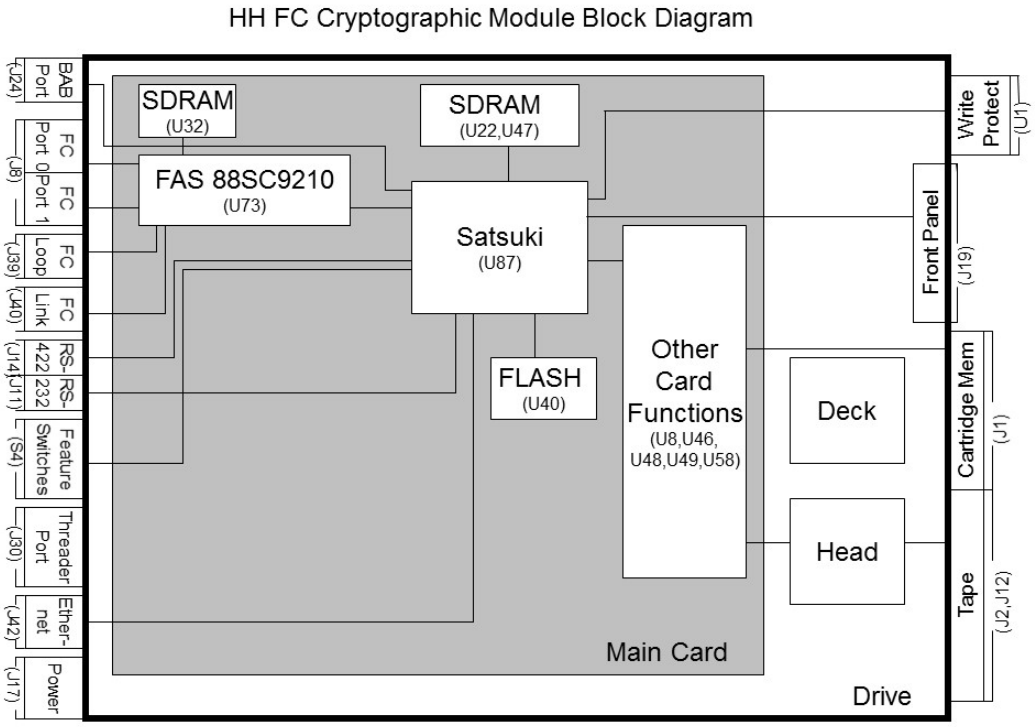

Figure 1a: LTO-7 and LTO-8 Half-High Fibre Channel Drive Block Diagram

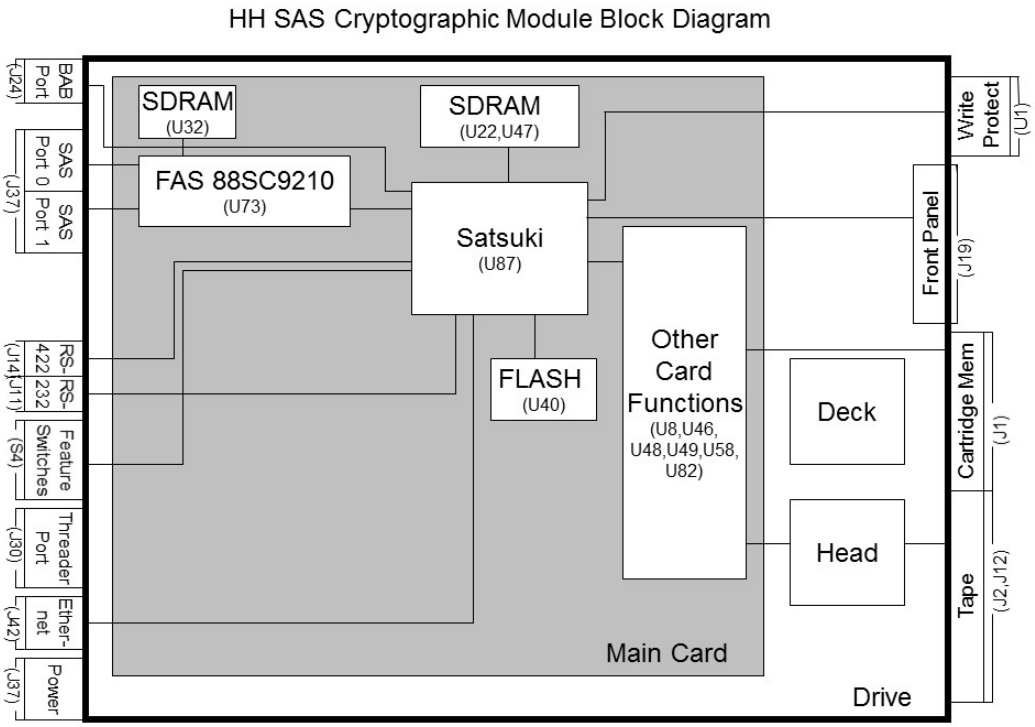

Figure 1b: LTO-7 and LTO-8 Half-High SAS Drive Block Diagram

The LTO-7 and LTO-8 tape drives have 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-7 and LTO-8 tape drives automatically perform 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 key manager, such as the HPE StoreEver MSL Encryption Kit or HPE StoreEver ESKM, 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-7 and LTO-8 tape drives to maintain FIPS 140 validation.

There is only one supported configuration for the LTO-7 and LTO-8 tape drives in the approved mode of operation. This is **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 Ultrium LTO-7 or LTO-8 Tape Drive Technical Reference Manual.

The LTO-7 or LTO-8 tape drive 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 2: Reported Values Indicating Approved Modes of Operation

Required Fields	**T10 SCSI Encryption**	
	Via library interface	Via host interface
Key Path (Manager Type) (from VPD) Mode Page 25h, byte 21, bits 7-5	000b	101b
In-band Key Path (Manager Type) Override Mode Page 25h, byte 21, bits 4-2	000b	000b
Indirect Key Mode Default Mode Page 25h, byte 22, bit 4	0b	0b
Key Scope Mode Page 25h, byte 23, bits 2-0	000b	000b
Encryption Method Mode Page 25h, byte 27	60h	50h

Certain commands are prohibited while in the approved modes of operation. In the T10 SCSI encryption configuration, all Mode Select commands to Mode Page 30h, Subpage 20h and all subpages of Mode Page 25h are prohibited on the host interface.

Table 3: Host Interface Mode Select Eligibility of Mode Page 30h, Subpage 20h and Mode Page 25h Subpages

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

Loading a FIPS 140-2 validated drive microcode level and configuring the drive for one of the approved modes of operation initializes the LTO-7 or LTO-8 tape drive 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-7 and LTO-8 tape drives support multi-initiator environments, but only one initiator may access cryptographic functions at any given time. Therefore the LTO-7 and LTO-8 tape drives do not support multiple concurrent operators.

The LTO-7 and LTO-8 tape drives implement 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.

[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.

The LTO-7 and LTO-8 tape drives operate as a stand-alone tape drive and have no direct dependency on any specific operating system or platform for FIPS approved operating modes, but do have requirements for:

- Key Manager/Key Store attachment
- Drive Configuration

The following criteria apply to the usage environment:

- Drive Configuration requirements
  - The LTO-7 or LTO-8 tape drive must be configured in the approved mode of operation.
  - The LTO-7 or LTO-8 tape drive must have the FIPS 140-2 validated drive firmware level loaded and operational.
  - In T10 SCSI encryption mode via the library interface, the LTO-7 or LTO-8 tape 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-7 and LTO-8 tape drives 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 4: Ports Common to All Host Interface Types

LTO-7 and LTO-8 tape 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	Data Input Data Output Control Input Status Output	Yes	▪ Crypto: Inputs protected keys from the key manager in 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.
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 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-7 and LTO-8 tape drive
Front Panel Amber LED	Status Output	None	▪ Displays status
Front Panel Green LED	Status Output	None	▪ Displays status
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 5: Fibre Channel-Specific Host Interfaces Ports

LTO-7 and LTO-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 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 6: SAS-Specific Host Interfaces Ports

LTO-7 and LTO-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 T10 SCSI encryption mode via the host interface ▪ 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-7 and LTO-8 tape drives support both a Crypto Officer role and a User role, and use basic cryptographic functions to provide higher level services. For example, the LTO-7 or LTO-8 tape 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-7 and LTO-8 tape drives provide 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-7 or LTO-8 tape drive. Under these circumstances the LTO-7 or LTO-8 tape 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-7 and LTO-8 tape drives enforce 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 7: Provided Services Applicable to All Modes of Operation

Service	Interface(s)	Description	Inputs	Outputs	Role
General SCSI commands	- Host	As documented in the HPE Ultrium LTO-7 or LTO-8 Tape Drive Host Interface Guide	See description	See description	User
General Library Interface commands	- Library	As documented in the HPE Automation Integration Guide	See description	See description	User
Load tape	- Host/Library	Load tape can be performed by commands sent over the host or library interface	See description	Green LED flashes while the load is in progress	User
Unload tape	- Host/Library	Unload tape can be performed via commands over the host or library interface	See description	Green LED flashes while unload is in progress.	User
Show Status (Visual Indicators)	- Front Panel LEDs	Visual indicators that an encryption operation is currently in progress may be monitored on the front panel	From LTO-7 and LTO-8 tape 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-7 and LTO-8 tape drive operating system	Vital Product Data (VPD)	User
Key Zeroization	- Host	Zeroes all private plaintext keys in the LTO-7 or LTO-8 tape drive via a Send Diagnostic command with Diagnostic ID EFFFh	Send Diagnostic command specifying the Key Zeroization diagnostic	Send Diagnostic command status	Crypto Officer
Firmware Load	- Host	Load new firmware to the module	New firmware	Load test indicator	Crypto Officer

Table 8: Provided Services Applicable to T10 SCSI Encryption

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

[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 refer to the HPE Ultrium LTO-7 or LTO-8 Tape Drives Technical Reference Manual.

Service	Interface (s)	Description	Inputs	Outputs	Role
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
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 refer to the HPE Ultrium LTO-7 or LTO-8 Tape Drives Technical Reference Manual.

3.5 Physical Security

The LTO-7 and LTO-8 tape 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-7 and LTO-8 tape drives require no preventative maintenance, and field repair is not performed for the units. 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.

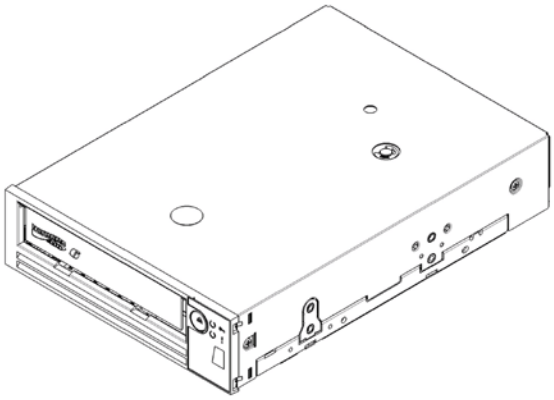

Figure 2a: Front View of LTO-7 and LTO-8 Half-High Drive Brick

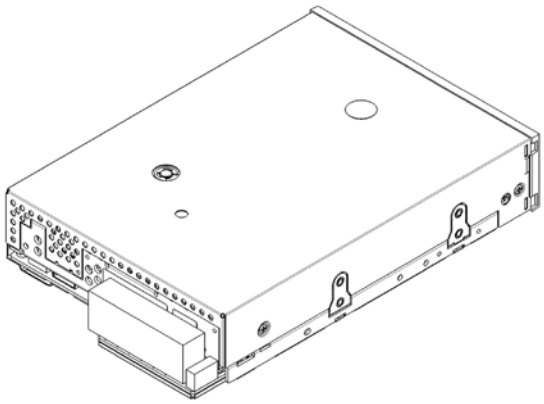

Figure 2b: Rear View of LTO-7 and LTO-8 Half-High Fibre Channel Drive Brick

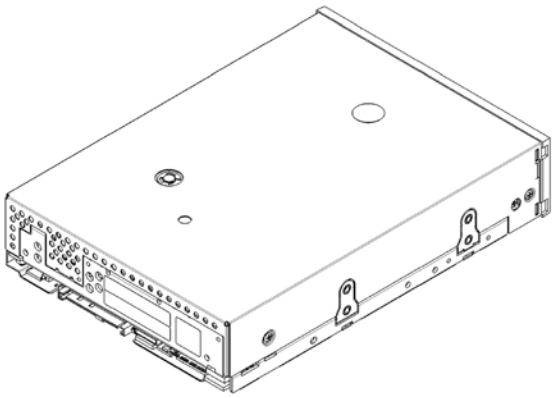

Figure 2c: Rear View of LTO-7 and LTO-8 Half-High SAS Drive Brick

3.6 Cryptographic Algorithms and Key Management

3.6.1 Cryptographic Algorithms

The LTO-7 and LTO-8 tape drives support 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 9: 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-7 and LTO-8 tape drive critical security parameters (CSPs) and non-critical security parameters.

Table 10: 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	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
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

[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

Additional notes on key management:

- Secret and private keys are never output from the LTO-7 and LTO-8 tape drives in plaintext form.
- Secret keys may only be imported to the LTO-7 and LTO-8 tape drive in encrypted form.
- Zeroization behavior outlines in **Table 11**.

Table 11: 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 Zeroization	W	W	W	W	W	W	W	W	W	
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										

	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
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-7 and LTO-8 tape drives perform 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 12: Self-Tests

Function Tested	Self-Test Type	Implementation	Failure Behavior
AES-ECB	Power-up	KAT performed for Encrypt and Decrypt	Errorcode 0x1130 reported
AES-GCM (256-bit keys)	Power-Up	KAT performed for Encrypt and Decrypt (256-bit)	Errorcode 0x1130 reported
DRBG	Power-Up	KAT performed	Errorcode 0x1133 reported
SHA-1	Power-Up	KAT performed	Errorcode 0x1131 reported
SHA-256	Power-Up	KAT performed	Errorcode 0x1131 reported
SHA-512	Power-Up	KAT performed	Errorcode 0x1131 reported

Function Tested	Self-Test Type	Implementation	Failure Behavior
RSA Sign KAT and Verify KAT	Power-Up	KAT performed	Errorcode 0x1131 reported
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)	Errorcode 0x112E reported
DRBG	Conditional: When a random number is generated	Continuous random number generator test performed.	Errorcode 0x1133 reported
DRBG	Conditional: When random numbers are generated	SP800-90A DRBG Health Tests (Instantiate, Generate and Reseed)	Errorcode 0x1133 reported
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)	Errorcode 0x1133 reported
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 errorcode 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-7 and LTO-8 tape drives support 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-7 or LTO-8 tape drive checks the interface on which the bypass request was received for transmission errors. Then the LTO-7 or LTO-8 tape drive checks the value of the received bypass instruction. For T10 SCSI Encryption, the Encryption Mode and Decryption Mode fields of Security Protocol Out Security Protocol 20h, Security Protocol Specific 0010h determine if the bypass capability is enabled.

3.7 Design Assurance

LTO-7 and LTO-8 tape drive release parts are maintained under the HPE Production Change Order (PCO) system. All components are assigned a part number and revision and may not be changed without a PCO.

The following table shows the certified configuration for each host interface of the LTO-7 and LTO-8 tape drives:

Table 13: Certified Configurations

Drive model	Hardware Part Number	Firmware Version	Firmware Image
HPE LTO-7 HH FC	AQ308A#103	G986	LTO_15000_FC_G986_MSL_S.frm
HPE LTO-7 HH SAS	AQ303A#103	G986	LTO_15000_SAS_G986_MSL_S.frm
HPE LTO-8 HH FC	AQ338A#103	J4DB	LTO_30750_FC_J4DB_MSL_S.frm
HPE LTO-8 HH SAS	AQ333A#103	J4DB	LTO_30750_SAS_J4DB_MSL_S.frm

3.8 Mitigation of other attacks

The LTO-7 and LTO-8 tape drives do not claim to mitigate other attacks.