Hewlett Packard
Enterprise

HPE LTO-6 Tape Drive
Level 1 Non-Proprietary Security Policy

Version: 10

Revision Date: 10 March 2017

Contents

Tables

Figures

1 Module Overview

The HPE LTO-6 Tape Drive sets new standards for capacity, performance, and manageability. The HPE LTO-6 represents HPE's sixth-generation of LTO tape drive technology capable of storing up to 6.25 TB per cartridge while providing enterprise tape drive monitoring and management capabilities with HPE TapeAssure and AES 256-bit hardware data encryption, easy-to-enable security to protect the most sensitive data and prevent unauthorized access of tape cartridges. Capable of data transfer rates up to 400MB/sec, HPE's exclusive Data Rate Matching feature further optimizes performance by matching speed of host to keep drives streaming and increase the reliability of the drive and media. HPE LTO-6 drives are designed for server customers in direct attached storage (DAS) environments where hard disk and system bottlenecks can impede data transfer rates. The HPE LTO-6 provides investment protection with full read and write backward support with LTO-5 media, and the ability to read LTO-4 cartridges. By nearly doubling the capacity of previous generation Ultrium drives, HPE customers now require fewer data cartridges to meet their storage needs, significantly reducing their IT costs and increasing their ROI.

The HPE LTO-6 Tape Drive (hereafter referred to as “the module”) is a multi-chip standalone module composed of hardware and firmware components, providing cryptographic services to a host.

The boundary of the module is the enclosure of the tape drive. The tape media, medium auxiliary memory, and cartridge fall outside the cryptographic boundary of the module.

No components of the tape drive are excluded from the cryptographic boundary.

Figure 1 – Half-height Internal Tape Drive (HPE LTO-6 HW versions AQ288D #103 and AQ298C #103)

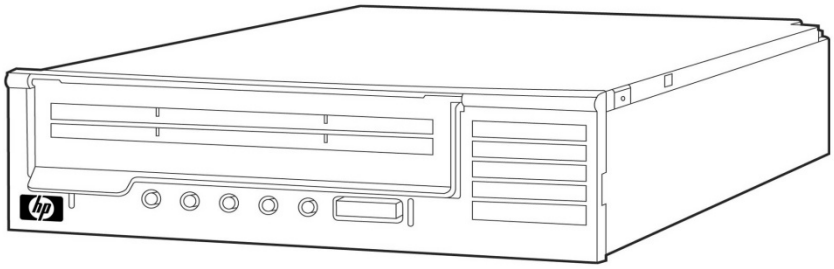
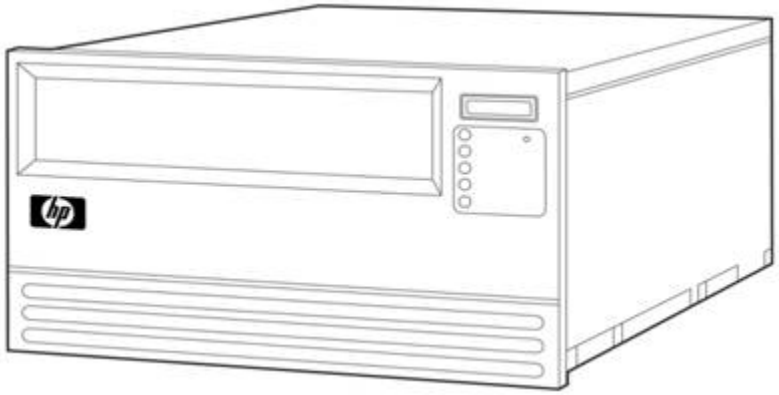


Figure 2 – Full-height Internal Tape Drive (HPE LTO-6 HW version AQ278A #912)



The HPE LTO-6 Tape Drive has three (3) variants for this revalidation:

Table 1 – Module Variants

Variant	Hardware Version	Firmware Version	Description
HPE LTO-6 Full-height with 8Gb/s Fibre Channel	AQ278A #912	J5SW	For use in HPE ESLG3 tape libraries
HPE LTO-6 Half-height with 6Gb/s SAS	AQ288D #103	35PW	For use in HPE MSL G3 tape libraries
HPE LTO-6 Half-height with 8Gb/s Fibre Channel	AQ298C #103	25MW	For use in HPE MSL G3 tape libraries

With all three variants, all cryptographic functions, roles, and services are identical between each variant. Only non-security-relevant differences exist between the variants.

Host data is provided to the module in plaintext, and the security of that data while it is outside the module is beyond the scope of the security provided by the module.

Figure 3 depicts a block diagram of the HPE LTO-6 Tape Drive hardware components, with the cryptographic boundary shown. The major blocks of the HPE LTO-6 Tape Drive hardware are:

- Memory: RAM, DRAM, EEPROM and Flash
- CPU: Four ARM 9 processors (two perform cryptographic operations), one included inside Servo Electronic ASIC
- TRNGs (NDRNG)
- Motors, Sensors
- Read/Write Heads and Channels
- Host Interface assembly

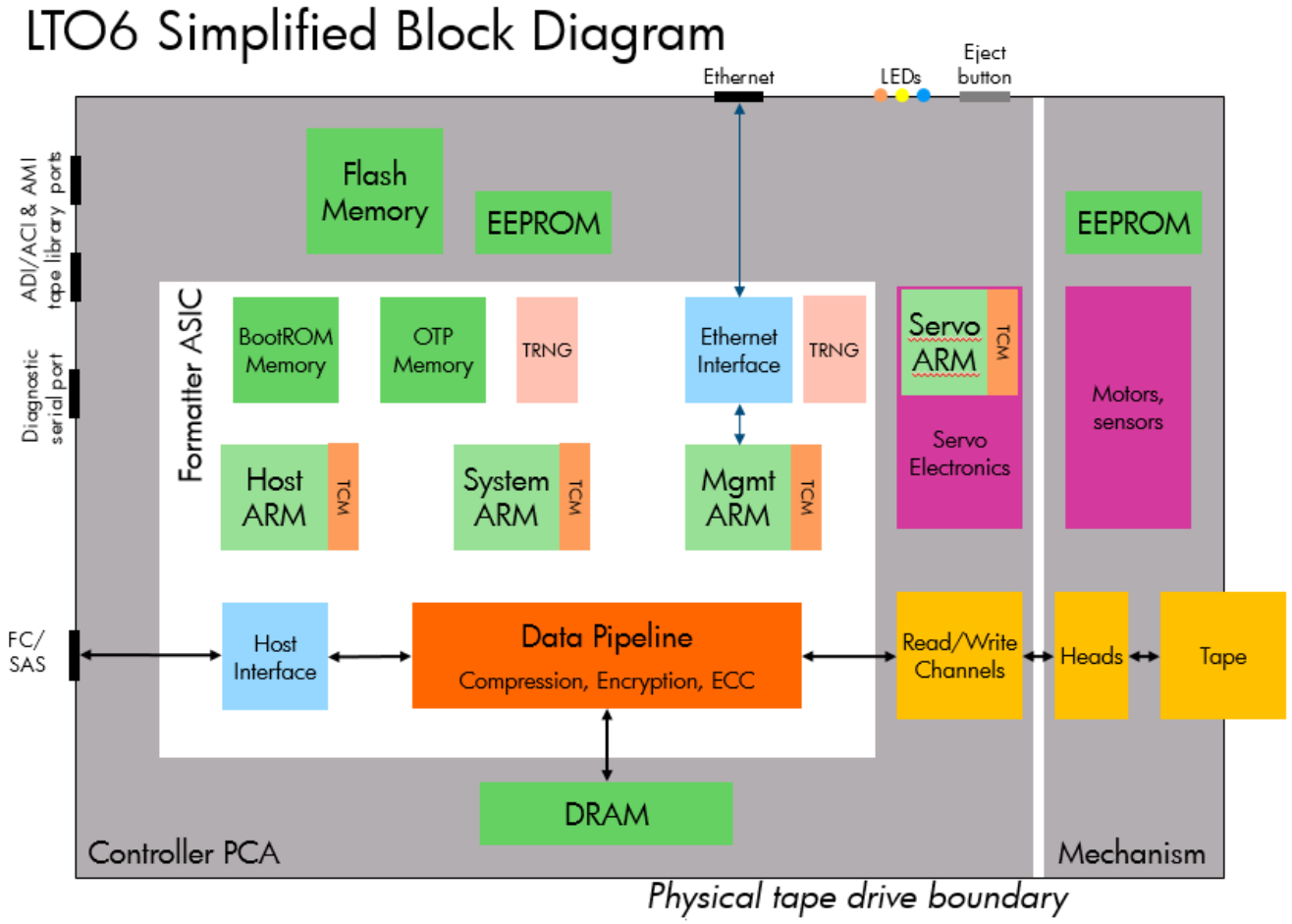


Figure 3 – HPE LTO-6 Tape Drive Block Diagram

2 Security Level

The cryptographic module meets the overall requirements applicable to Level 1 security of FIPS 140-2.

Table 2 – Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	1
Module Ports and Interfaces	1
Roles, Services and Authentication	1
Finite State Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A

3 Modes of Operation

3.1 FIPS Approved Mode of Operation

Following successful power up initialization according to Section 8 below, the module will enter FIPS Approved mode. FIPS mode can be confirmed by issuing a SECURITY PROTOCOL IN command specifying the Security Configuration security protocol and the Status page. The security mode enabled (SME) bit will be set to '1' and the FIPS LEVEL field will be set to '1'.

3.2 Non-FIPS Mode of Operation

Not applicable – the module does not have a non-FIPS mode of operation.

3.3 Approved and Allowed Algorithms

The cryptographic module supports the following FIPS Approved algorithms.

Table 3 – FIPS Approved Algorithms Used in Current Module

Algorithm & References	Mode/Method/Strength	CAVP Cert. #
AES [FIPS 197]	ECB; 256 bits; decrypt (supports key wrap)	1442
AES [FIPS 197], [SP 800-38D]	ECB, CTR, GCM; 256 bits	2189
AES [FIPS 197]	CBC, ECB, GCM; 128, 256 bits	3534
AES [SP 800-38F]	AES Key Wrap (AES-256)	3535
CVL [SP 800-135]	TLS 1.0/ 1.1/ 1.2 (SHA-256 and SHA-384)	588
DRBG [SP 800-90A]	CTR_DRBG AES-256	889
HMAC [FIPS 198]	HMAC (w/SHA-1, -224, -256, -384, -512)	2258
RSA [FIPS 186-4]	Signature verification only; 2048 bits (SigGen tested but not used)	1128
RSA [FIPS 186-4]	RSASSA-PKCS1-V1_5; 2048-bit sign / 1024-, 2048-, 3072-bit verify; RSASSA-PSS; 2048-bit verify (FIPS 186-2 supported but not used)	1821
SHS [FIPS 180]	SHA-256	1897
SHS [FIPS 180]	SHA-1, -224, -256, -384, -512	2913

When configured as per Section 8 below, only FIPS Approved ciphersuites are allowed within TLS. Those are: TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA256, and TLS_RSA_WITH_AES_256_CBC_SHA256. This protocol has not been reviewed or tested by the CAVP and CMVP.

The cryptographic module supports the following non-FIPS Approved algorithms which are allowed for use in FIPS mode.

Table 4 – FIPS Allowed Algorithms Used in Current Module

FIPS Allowed Algorithm
RSAES-OAEP (w/SHA-256) Key wrapping; key establishment methodology provides 112 bits of encryption strength.
HW NDRNGs (Qty. 2) – Used to seed the Approved DRBG
MD5 within TLS

4 Ports and Interfaces

The HPE LTO-6 Tape Drive is a multi-chip standalone module with ports and interfaces as shown below.

Table 5 – HPE LTO-6 Tape Drive Pins and FIPS 140-2 Ports and Interfaces

Full Height (Fibre)	Half Height (Fibre)	Half Height (SAS)	FIPS 140-2 Designation	Name and Description
X	X		Power input	Power connector (12VDC, 5VDC, ground)
X	X		Data input, control input, data output, status output	Fibre Channel (FC) host interface connectors (Qty. 2)
		X	Status output	6 pin external fan support connector
		X	Data Output	9 pin active SAS Management connector
		X	Data input, control input, data output, status output, power input	Serial Attached SCSI (SAS) host interface connector
X	X	X	Data output (to tape medium)	Tape write heads
X	X	X	Data input (from tape medium)	Tape read heads
X	X	X	Control input, status output	16 pin ADI/ACI connector
X	X	X	Status output	Host LED connector (Qty. 2)
X	X	X	Control input, status output	4 pin Automation Management Interface (AMI) or Diagnostic Protocol serial port
X	X	X	Data input, control input, status output	10 pin iADT (Ethernet) connector
X	X	X	Control input	Eject button on bezel to manually eject tape cartridge
X			Control input	Reset switch accessed through a pinhole immediately below the right-hand end of the eject button
X	X	X	Status output	Five LED indicators: “Ready,” “Drive Error,” “Tape Error,” “Clean,” and “Encryption”

5 Identification and Authentication Policy

5.1 Assumption of Roles

The module supports two (2) distinct operator roles, Cryptographic Officer (CO) and User. An operator implicitly assumes a role based on the service performed. The module does not support authentication.

The module does not provide a maintenance role or bypass capability.

Table 6 – Roles and Required Identification and Authentication

Role	Description	Authentication Type	Authentication Data
CO	This role can set security parameters.	N/A	N/A
User	This role has access to basic functionality offered by the module.	N/A	N/A

6 Access Control Policy

6.1 Services

Table 7 – Authorized Services

Service	Description
Set private security parameters	SCSI commands to set private security parameters
Zeroize	SCSI commands to overwrite all plaintext CSPs within the module
Upgrade module firmware	SCSI command to write firmware
Write data to tape	SCSI command to write data to tape
Read data from tape	SCSI command to read data from tape
Load/unload tape	SCSI command to load or unload tape cartridge to/from the drive
Verify tape data	SCSI command to verify integrity of data on tape
Erase tape data	SCSI command to erase all data on tape

6.2 Unauthorized Services

The cryptographic module supports the following services for which a role is not required to be assumed:

Table 8 – Unauthorized Services

Service	Description
Hard Reset	Power cycle, Reset button, or SCSI command to reboot (initiates self-tests)
Get public security parameters	Read only access to public security parameters
Status commands	SCSI or diagnostic commands used to report drive configuration
Reservation commands	SCSI commands to control access to the drive
Tape motion commands	SCSI commands to alter the logical position of the tape
Tape control and configuration commands	SCSI commands to set and get non-security related drive parameters
Logging commands	SCSI or diagnostic commands to view or clear statistics, counters, or logs

6.3 Definition of Critical Security Parameters (CSPs)

The module contains the following CSPs:

Table 9 – Secret/Private Keys and CSPs

Key Name	Type	Description
Drive Root Key (DRK)	AES 256-bit	Used to encrypt the CSPs which are stored in EEPROM.
Drive Private Key (DRPV)	RSA 2048-bit	Used to authenticate Transport Layer Security (TLS) connection between host and module.
Key Encryption Key (KEK)	AES 256-bit	Used to encrypt the data encryption key.
TLS Pre-Master Secret (TLSP)	Pre-Master Secret	Used by TLS to establish the session keys.
TLS HMAC Key (TLSH)	HMAC	TLS HMAC Key to provide data integrity over TLS session. (64 to 128 bytes)
TLS Encryption Key (TLSK)	AES 128-bit or 256-bit	Used to provide data protection over TLS session.
Data Encryption Key (DEK)	AES 256-bit	Used to encrypt data written to tape and decrypt data read from tape.
Seed and Seed Keys (S/SK)	Seed and Seed Key	Used to initialize the Approved DRBG.(IG 7.14 1(a) applies; minimum entropy of 191 bits provided)
VNK (V and Key)	DRBG internal state data	Internally generated using DRBG

6.4 Definition of Public Keys

The module contains the following public keys:

Table 10 – Public Keys

Key Name	Type	Description
Root CA public key (RTPK)	RSA 2048-bit	Forms the basis of the “trust tree”. Used to authenticate Transport Layer Security (TLS) connection between host and module and to authenticate public keys in whitelist.
Management Host public key (MHPK)	RSA 2048-bit	A trusted Host public key. Used to authenticate management host to drive to permit installing and deleting certificates and changing secure mode enabled and level.

Key Name	Type	Description
Client CA Public Key (CLPK)	RSA 2048-bit	A trusted CA public key. Used to authenticate Transport Layer Security (TLS) connection between clients and module.
Drive Public Key (DRPK)	RSA 2048-bit	Used to authenticate Transport Layer Security (TLS) connection between host and module.
Firmware OTP Public Key, also known as "HPE Public Key" (HPPK)	RSA 2048-bit	A 2048-bit RSA public key used to check signature of boot loader firmware at startup.
Firmware Public Key (IPK)	RSA 2048-bit	Used to authenticate firmware upgrades by checking the signature on any new firmware image before installing it.
[1] These keys may be present in Level 1 but are not used.		

6.5 Definition of CSPs Modes of Access

Table 11 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as:

- **G** = Generate: The module generates the CSP.
- **R** = Read: The module reads the CSP. The read access is typically performed before the module uses the CSP.
- **W** = Write: The module writes the CSP. The write access is typically performed after a CSP is imported into the module, or the module generates a CSP, or the module overwrites an existing CSP.
- **Z** = Zeroize: The module zeroizes the CSP.

Table 11 – CSP Access Rights within Roles & Services

Role	Authorized Service	Mode	Cryptographic Key or CSP
CO	Set private security parameters	W Z G	CLPK DRK DRPK DRPV KEK MHPK RTPK
CO	Zeroize	Z	CLPK DRK DRPK DRPV MHPK RTPK

Role	Authorized Service	Mode	Cryptographic Key or CSP
User/CO	Upgrade module firmware	R, W	IPK
User	Write data to tape	G, W	DEK
User	Read data from tape	R	DEK
User	Load/unload tape	Z	DEK KEK
User	Verify tape data	R	DEK
User	Erase tape data	N/A	N/A
N/A	Hard reset	Z	DRPV KEK DEK MHPK S/SK TLSP TLSH TLSK VNK HPPK
N/A	Get public security parameters	R	CLPK DRPK IPK MHPK RTPK
N/A	Status commands	N/A	N/A
N/A	Reservation commands	Z	DEK KEK
N/A	Tape motion commands	N/A	N/A
N/A	Tape control and configuration commands	N/A	N/A
N/A	Logging commands	N/A	N/A

7 Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the HPE LTO-6 Tape Drive does not contain a modifiable operational environment.

The module includes a firmware load service to support necessary updates. New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into this module is out of the scope of this validation and require a separate FIPS 140-2 validation.

8 Security Rules

The HPE LTO-6 Tape Drive design corresponds to the HPE LTO-6 Tape Drive security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 1 module.

In order to operate the HPE LTO-6 product in a FIPS approved mode at Level 1:

a) Root CA and Device certificates must be installed (as per the Ultrium 6 Security Configuration Protocol specification), and secure mode must be enabled (by sending a Security Configuration Control page with the SME bit set to1) with FIPS level set to 1; and
b) Encrypt mode must be enabled before data is written to or read from tape; and
c) Encryption keys may be passed to the drive in one of two ways – either over authenticated TLS or over the serial ADT port using Device Server Public Key Wrapping.

If either the secure mode is set to disabled or the Level is changed to a value other than 1, then it will no longer be operating in compliance with FIPS Level 1.

1. The cryptographic module shall provide two (2) distinct operator roles. These are the User role and the Cryptographic Officer role.
2. The cryptographic module shall perform the following tests

A. Power up Self-Tests

1. Cryptographic algorithm tests
   a. AES Encrypt/Decrypt Known Answer Test (AES Cert. #1442)
   b. AES GCM Encrypt/Decrypt Known Answer Tests (AES Cert. #2189)
   c. SP 800-38F AES Key Wrap/Unwrap Known Answer Tests (AES Cert.#3535)
   d. RSA Verify Known Answer Test (tested as part of firmware integrity test) (RSA Cert. #1128)
   e. SHA-256 Known Answer Test (tested as part of firmware integrity test) (SHA Cert. #1897)
   f. AES Encrypt/Decrypt Known Answer Test (AES Cert.#3534)
   g. AES GCM Known Answer Test (AES Cert. #3534)
   h. RSA Sign/Verify Known Answer Test (RSA Cert. #1821)
   i. SHA-1, -224, -256, -384, -512 Known Answer Tests (SHA Cert. #2913)
   j. HMAC (w/ SHA-1, -224, -256, -384, -512) Known Answer Tests (HMAC Cert. #2258)
   k. CTR_DRBG Known Answer Test – Includes SP800-90 Health Checks (DRBG Cert. #889)
   l. RSAES_OAEP (w/ SHA-256) Decrypt KAT

2. Firmware Integrity Test (RSA 2048 signature verification)

B. Critical Functions Tests – N/A

C. Conditional Self-Tests

1. Continuous Random Number Generator (RNG) test – performed on NDRNGs and DRBG
2. RSA Sign/Verify Pairwise Consistency Test
3. Firmware Load Test (RSA 2048 bit signature verification)

3. The operator shall be capable of commanding the module to perform the power-up self-test by cycling power or resetting the module. If the module passes self-tests successfully, the 'Ready' LED will light solid green. If any of the above self-tests fail, the module will enter an error state indicated by flashing 'Drive Error' and 'Tape Error' LEDs, combined with the Encryption LED lit solid blue. The only actions possible in this state are to reset the module (which will repeat the self-tests), or load new firmware.
4. Power-up self-tests do not require any operator action.
5. Data output shall be inhibited during key generation, self-tests, zeroization, and error states.
6. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
7. The module ensures that the seed and seed key inputs to the Approved DRBG are not equal.
8. The module does not support a maintenance interface or role.
9. The module does not support manual key entry.
10. The module does not have any external input/output devices used for entry/output of data.
11. The module does not output plaintext CSPs.
12. The module does not output intermediate key values.

9 Physical Security Policy

9.1 Physical Security Mechanisms

The multi-chip standalone module is production quality containing standard passivation.

10 Mitigation of Other Attacks Policy

No claim is made that the module will mitigate attacks outside of those required by the FIPS 140-2 Level 1 validation.

11 References

[FIPS 140-2] FIPS Publication 140-2 *Security Requirements for Cryptographic Modules*

Ultrium 6 Security Configuration Protocol

12 Definitions and Acronyms

ACI – Automation Controller Interface

ADI – Automation Drive Interface

ADT – Automation/Drive Interface Transport Protocol

AES – Advanced Encryption Standard

AMI – Automation Management Interface

CBC – Cipher Block Chaining

CSP – Critical Security Parameter

CTR_DRBG – DRBG using an approved block cipher algorithm

DRBG – Deterministic Random Bit Generator

ECB – Electronic Code Book

FIPS – Federal Information Processing Standard

GCM – Galois Counter Mode

HMAC – Hash-based Message Authentication Code

iADT – Internet ADT transport protocol (port 4169/tcp)

iADT-TLS – iADT over TLS transport protocol (port 9614/tcp)

iAMI – Internet AMI port

KAT – Known Answer Test

MAC – Message Authentication Code

OTP – One Time Programmable Memory

PKCS – Public Key Cryptography Standard

RFC – Request for Comments

RNG – Random Number Generator

ROI – Return on Investment

RSA – Rivest Shamir Adelman

RSAES-OAEP – RSA Encryption Scheme / Optimal Asymmetric Encryption Padding

RSASSA-PSS – RSA Signature Scheme with Appendix / Probabilistic Signature Scheme

SAS – Serial-Attached SCSI

SCSI – Small Computer Systems Interface

SHA – Secure Hash Algorithm

SHS – Secure Hash Standard

SSL – Secure Socket Layer

TLS – Transport Layer Security

TRNG – True Random Number Generator