HP LTO-6 Tape Drive
Level 2 Security Policy

Version: 9

Hewlett-Packard Company

Revision Date: 14 November 2013

Contents

Tables

Figures

1 Module Overview

The HP LTO-6 Tape Drive sets new standards for capacity, performance, and manageability. The HP LTO-6 represents HP'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 HP 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, HP'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. HP 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 HP 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, HP customers now require fewer data cartridges to meet their storage needs, significantly reducing their IT costs and increasing their ROI.

The HP 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.

The following components have been excluded from the requirements of FIPS 140-2:

- Power supply components
- Passive components (resistors, capacitors, etc.)
- Mechanical components responsible for tape movement

Figure 1 – Half-height Internal Tape Drive (HP LTO-6)

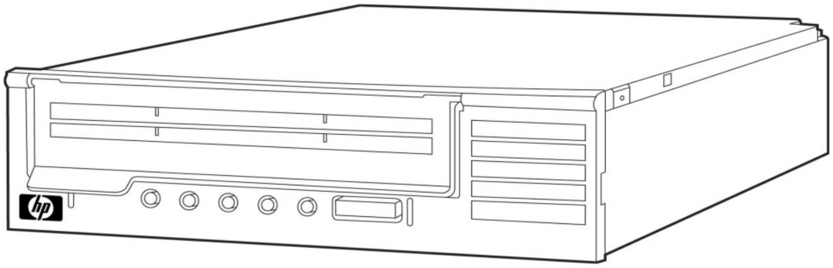
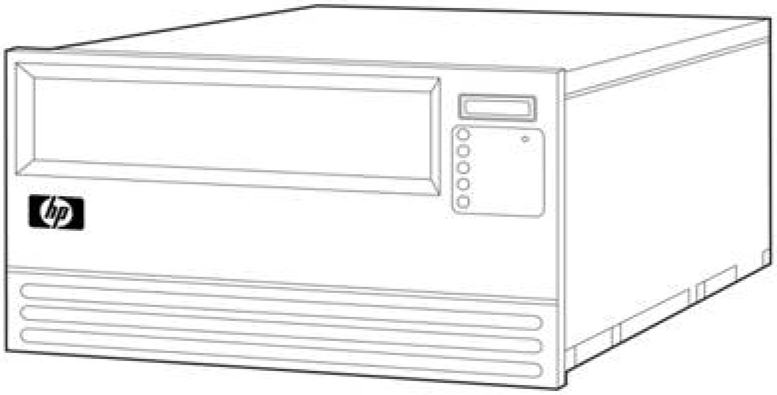


Figure 2 – Full-height Internal Tape Drive (HP LTO-6)



The HP LTO-6 Tape Drive has four variants for this validation:

Table 1 – Module Variants

Variant	Hardware Version	Firmware Version	Description
HP LTO-6 Full-height with 8Gb/s Fibre Channel	AQ278A #912	J2AW	For use in HP ESLG3 tape libraries
HP LTO-6 Full-height with 8Gb/s Fibre Channel	AQ278C #704	J2AS	For use in HP EML E-Series tape libraries
HP LTO-6 Half-height with 6Gb/s SAS	AQ288D #103	32AW	For use in HP MSL G3 tape libraries
HP LTO-6 Half-height with 8Gb/s Fibre Channel	AQ298C #103	22CW	For use in HP MSL G3 tape libraries

With all 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 HP LTO-6 Tape Drive hardware components, with the cryptographic boundary shown. The major blocks of the HP 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
- Motors, Sensors
- Read/Write Heads and Channels
- Host Interface assembly

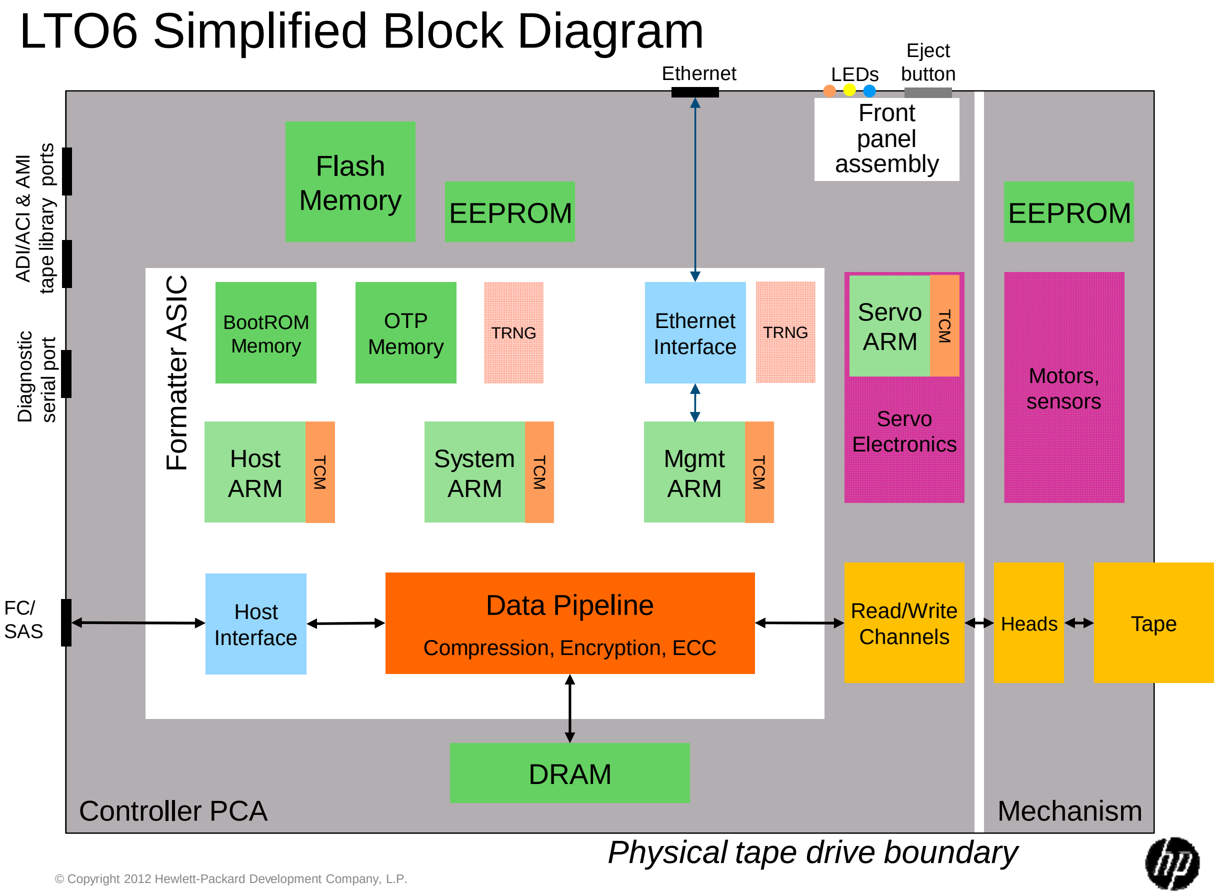


Figure 3 -- HP LTO-6 Tape Drive Block Diagram

2 Security Level

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

Table 2 – Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	2
Module Ports and Interfaces	2
Roles, Services and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	2
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 '2'.

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

FIPS Approved Algorithm	CAVP Cert. #
AES: ECB, CTR, GCM; 256 bits	2189
AES: ECB; 256 bits; decrypt	1442
RSA Signature verification only; 2048 bits	1128
SHA-256: RSA Signature verification only	1897
AES: CBC, ECB, 128, 256 bits	2190
AES: GCM; 128, 256 bits	2190
RSASSA-PKCS1-V1_5; 2048-bit sign / 1024-, 1536-, 2048-, 3072-bit verify	1129
RSASSA-PSS; 2048-bit verify	1129
SHA-1, -224, -256, -384, -512	1898
HMAC (w/SHA-1, -224, -256, -384, -512)	1342
SP 800-90 CTR_DRBG AES-256	256
CVL (SP 800-135rev1, vendor affirmed)	Vendor Affirmed

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.

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 unwrapping only, key establishment methodology provides 112 bits of encryption strength.
AES Key Wrap as per the NIST recommended Key Wrap Specification (AES Cert. #2189, key wrapping; key establishment methodology provides 256 bits of encryption strength)
HW NDRNGs (Qty. 2) – Used to seed the Approved DRBG
MD5 within TLS

4 Ports and Interfaces

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

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

Full Height (Fibre, both HW versions)	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	External fan support	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 connectors (Qty. 2)
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

Full Height (Fibre, both HW versions)	Half Height (Fibre)	Half Height (SAS)	FIPS 140-2 Designation	Name and Description
				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 distinct operator roles, User and Cryptographic Officer (CO). The cryptographic module enforces the separation of roles using role-based authentication.

The module supports multiple authentication mechanisms; which is used depends upon how the operator connects to the drive:

- Clients connecting on the Ethernet iADT-TLS or iAMI-TLS port (9614/tcp or 8614/tcp, respectively) using authenticated TLS are authenticated to operate in the Crypto Officer and User roles.
- Hosts connecting on the host interface may use the Security Configuration Protocol to authenticate operation in the Crypto Officer and/or User roles. The authentication request is signed using the host's 2048-bit RSA private key; the corresponding public key used for verification must be in the authentication whitelist.
- Clients connecting on the Ethernet iADT or iAMI port (4169/tcp or 4168/tcp, respectively) may use the Security Configuration Protocol to present a certificate signed by a certificate authority whose certificate is present in the drive as either the Root CA Certificate or the Client CA Certificate. These clients are authenticated to operate in the Crypto Officer Role for purposes of managing certificates and whitelist public keys.
- All other operators may access only unauthenticated services.

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 and zeroize the module.	Role-based operator authentication	RSA 1024 or 2048 bit signature verification
User	This role has access to basic functionality offered by the module.	Role-based operator authentication	RSA 1024 or 2048 bit signature verification

Table 7 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
RSA 1024 or 2048 bit signature verification	The probability that a random attempt will succeed or a false acceptance will occur is 2^{-80} or 2^{-112}, which is less than 10^{-6}. In the worst case scenario, the module can verify 88,260 digital signatures within a one minute period based on processing restraints. With an RSA 1024 bit signature, the probability of successfully authenticating within a one minute period is then 88,260 * 2^{-80} which is less than 10^{-5}.

6 Access Control Policy

6.1 Services

Table 8 – Authenticated 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 Unauthenticated Services

The cryptographic module supports the following unauthenticated services:

Table 9 – Unauthenticated Services

Service	Description
Hard Reset	Power cycle, Reset button, or SCSI command to reboot
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 10 – Secret/Private Keys and CSPs

Key Name	Type	Description
Drive Root Key (DRK)	AES 256-bit	Used to encrypt 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
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

6.4 Definition of Public Keys

The module contains the following public keys:

Table 11 – 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.
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.
Public Key Whitelist (WLPK)	RSA 1024 or 2048-bit	Up to five public keys used to authenticate the CO and Users on the host interface. Each key is associated with bits indicating the authorized roles.
Firmware OTP public key, also known as “HP public key” (HPPK)	RSA 2048-bit	Used to authenticate firmware upgrades
Firmware public key (IPK)	RSA 2048-bit	Used to authenticate firmware upgrades by checking the signature on any new firmware image before installing it.

6.5 Definition of CSPs Modes of Access

Table 12 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 12 – 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 WLPK
CO	Zeroize	Z	CLPK DEK DRK DRPK DRPV KEK MHPK RTPK WLPK
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

Role	Authorized Service	Mode	Cryptographic Key or CSP
N/A	Hard reset	Z	KEK DEK MHPK S/SK TLSP TLSH TLSK
N/A	Get public security parameters	R	CLPK DRPK IPK MHPK RTPK WLPK
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 HP LTO-6 Tape Drive does not contain a modifiable operational environment.

8 Security Rules

The HP LTO-6 Tape Drive design corresponds to the HP 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 2 module.

In order to operate the HP LTO-6 Tape Drive in a FIPS approved mode at Level 2:

a) secure mode must be enabled by sending a Security Configuration Control page with the SME bit set to1, as specified in the Ultrium 6 Security Configuration Protocol specification
b) FIPS Level must be set to 2
c) authenticated TLS must be enabled by installing Root CA and Device certificates
d) one or more public keys must be entered in the whitelist
e) encrypt mode must be enabled when data is written to a tape or read from a tape. In addition, an encryption key must be provided in an approved manner.

If either the secure mode is set to disabled or the Level is changed to a value other than 2, then it will no longer be operating in compliance with FIPS Level 2.

1. The cryptographic module shall provide two distinct operator roles. These are the User role, and the Cryptographic Officer role.

2. The cryptographic module shall provide role-based authentication.

3. The cryptographic module shall clear previous authentications on power cycle.

4. When the module has not been placed in a valid role, the operator shall not have access to any cryptographic services.

5. The cryptographic module shall perform the following tests:

   A. Power up Self-Tests

      1. Cryptographic algorithm tests
         a. AES Encrypt/Decrypt Known Answer Tests
         b. AES GCM Known Answer Test
         c. RSA Verify Known Answer Test (tested as part of firmware integrity test)
         d. SHA-256 Known Answer Test (tested as part of firmware integrity test)
         e. AES Encrypt/Decrypt Known Answer Test (OpenSSL)
         f. AES GCM Known Answer Test (OpenSSL)
         g. RSA Sign/Verify Known Answer Test (OpenSSL)
         h. SHA-1, -224, -256, -384, -512 Known Answer Tests (OpenSSL)
         i. HMAC (w/ SHA-1, -224, -256, -384, -512) Known Answer Tests (OpenSSL)
         j. CTR_DRBG Known Answer Test (OpenSSL) – Includes SP800-90 Health Checks
         k. 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, 64 bits
2. RSA Sign/Verify Pairwise Consistency Test
3. Firmware Load Test (RSA 2048 bit signature verification)

6. 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 a flashing ‘Drive (Error)’ LED. The only actions possible in this state are to reset the module (which will repeat the self-tests), or load new firmware.
7. Power-up self-tests do not require any operator action.
8. Data output shall be inhibited during key generation, self-tests, zeroization, and error states.
9. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
10. The module ensures that the seed and seed key inputs to the Approved DRBG are not equal.
11. The module does not support a maintenance interface or role.
12. The module does not support manual key entry.
13. The module does not have any external input/output devices used for entry/output of data.
14. The module does not output plaintext CSPs.
15. 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. Module components are protected by an opaque, metal enclosure.

Tamper evidence is provided by 6 tamper seals for the full height drive, and 4 tamper seals for the half height drive that are applied during the manufacturing process. Please refer to Figures 4 through 6 for the correct placement of the labels. The tamper seals should be inspected once a month for evidence of tamper.

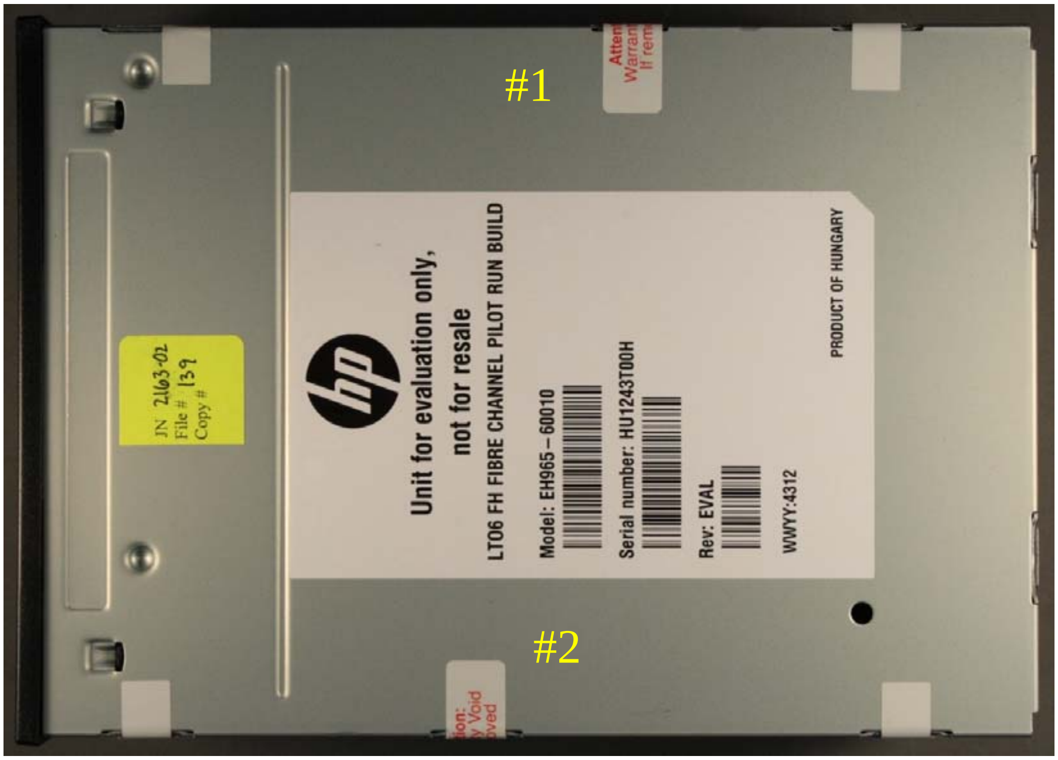


Figure 4 – Tamper Evident Seal Locations #1 & #2 Full-height Top

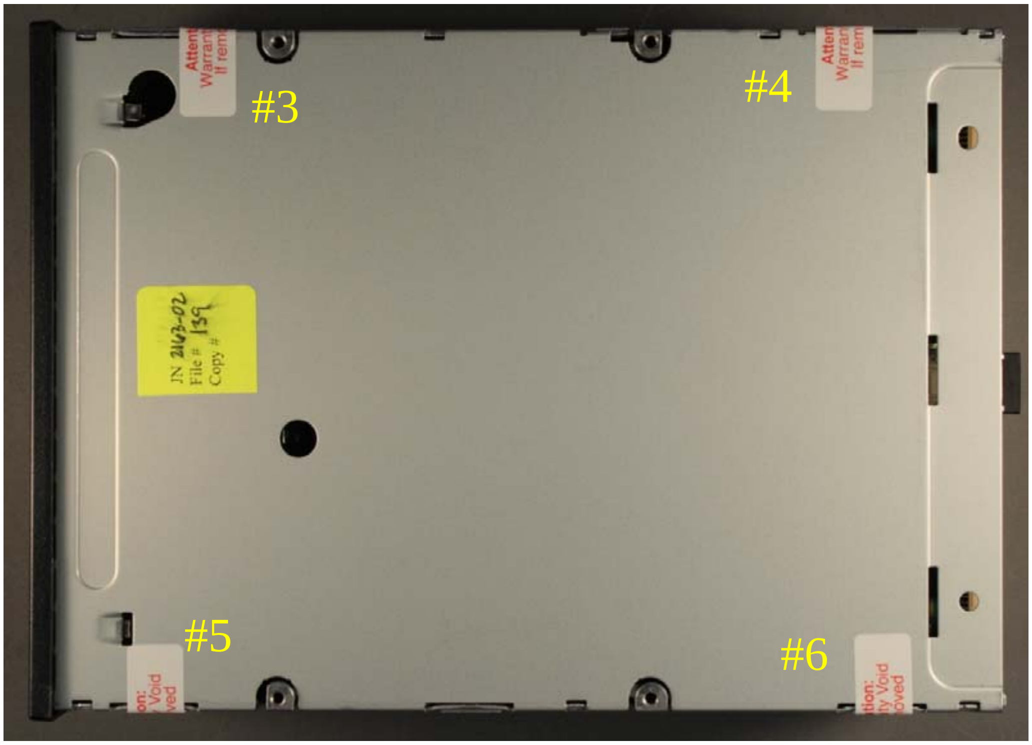


Figure 5 – Tamper Evident Seal Locations #3-6 Full-height bottom

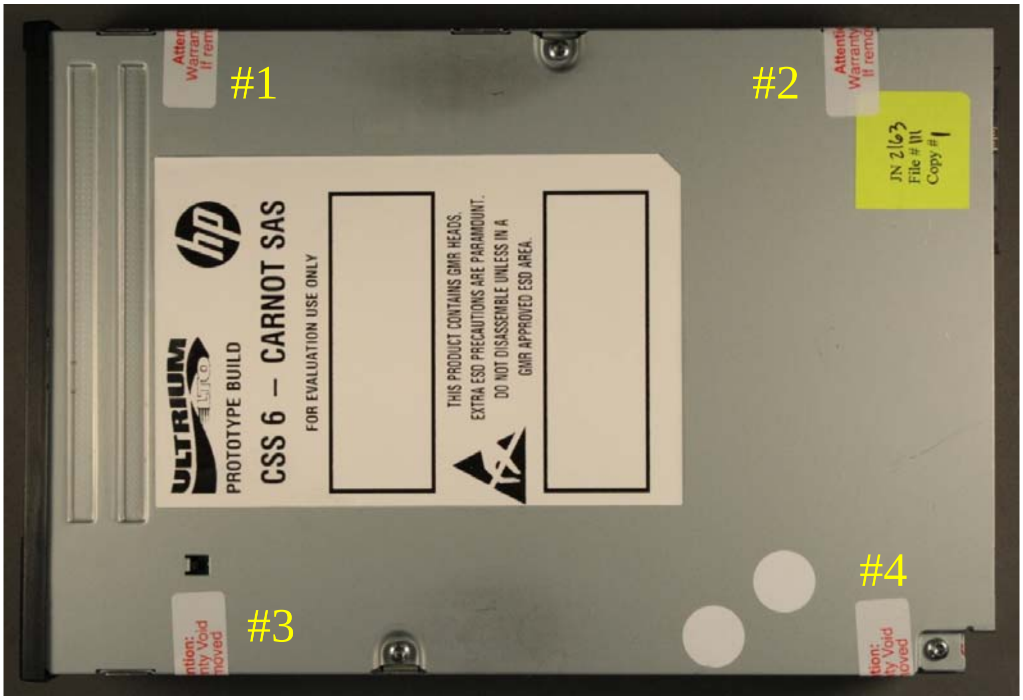


Figure 6 – Tamper Evident Seal Locations #1-4 Half-height Top

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 2 validation.

11 References

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

Ultrium 6 Security Configuration Protocol

12 Definitions and Acronyms

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

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