# HP LTO-5 Tape Drive

# FIPS 140-2 Non-Proprietary Security Policy

**Overall Level 1 Validation**

**Revision 001, 29 October 2010**

# Table of Contents

## Table of Figures and Tables

# 1 INTRODUCTION

## *1.1 Purpose*

This document is the non-proprietary FIPS 140-2 security policy for the HP LTO-5 product. This Security Policy details the secure operation of the HP LTO-5 as required in Federal Information Processing Standards Publication 140-2 (FIPS 140-2) as published by the National Institute of Standards and Technology (NIST) of the United States Department of Commerce.

## *1.2 References*

For more information on HP please visit http://www.hp.com/. For more information on NIST and the Cryptographic Module Validation Program (CMVP), please visit www.nist.gov/cmvp.

## *1.3 Document Organization*

This Security Policy document is one part of the FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence Document
- Finite State Machine
- Source Code Listing
- Other supporting documentation as additional references

This document outlines the functionality provided by the module and gives high-level details on the means by which the module satisfies FIPS 140-2 requirements. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Submission Documentation may be HP-proprietary or otherwise controlled and releasable only under appropriate non-disclosure agreements. For access to these documents, please contact HP.

# 2 The HP LTO-5 Tape Drive

HP LTO-5 Tape Drive (also referred to as HP LTO-5 or LTO-5 within this document) sets new standards for capacity, performance, and manageability. The HP LTO-5 represents HP's fifth-generation of LTO tape drive technology capable of storing up to 3TB 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 280MB/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-5 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-5 provides investment protection with full read and write backward support with LTO-4 media, and the ability to read LTO-3 cartridge. 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.

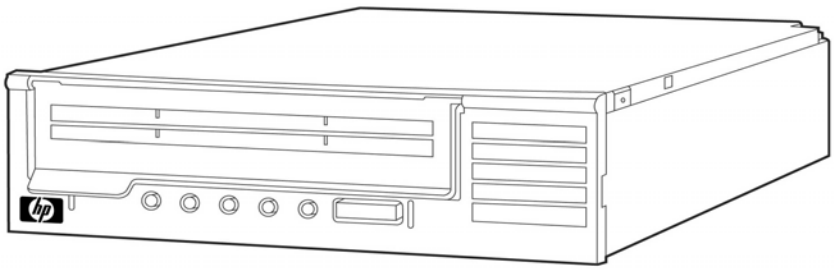
## *2.1 System overview*

The HP LTO-5 is a high-performance encrypting tape drive providing backup services to any connected host that is running appropriate software.

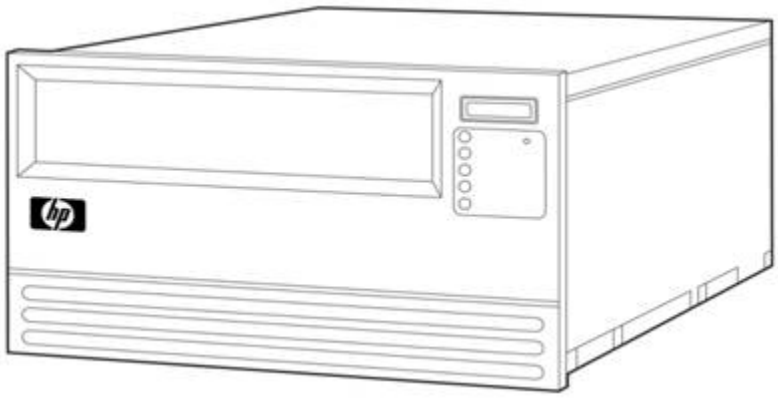
The HP LTO-5 is classified as a multi-chip standalone module for FIPS 140-2 purposes. It is a self-contained module containing both hardware and firmware components, providing cryptographic services to a host.

For the purposes of FIPS 140-2, the HP LTO-5 is validated at FIPS 140-2 Level 1.

The HP LTO-5 is available as either an external tape drive or an internal tape drive, although only the internal tape drive is subject to this validation. It is available as a full height and half height option:



Half-height Internal Tape Drive (HP LTO-5)



Full-height Internal Tape Drive (HP LTO-5)

**Figure 1 Internal Tape Drives**

**Internal Tape Drive:** The cryptographic boundary of the module is the enclosure of the internal tape drive. The tape media itself falls outside the cryptographic boundary of the module.

All hardware and firmware within the cryptographic boundary are subject to the security requirements of FIPS 140-2.

The HP LTO-5 has four hardware variants for this validation:

| Variant | Hardware version | Firmware version | Description |
|---|---|---|---|
| HP LTO-5 Full-height with 8Gb/s Fibre Channel | AQ273C #912 | I3BW | For use in HP ESL E-Series tape libraries |
| HP LTO-5 Full-height with 8Gb/s Fibre Channel | AQ273D #704 | I3AS | For use in HP EML E-Series tape libraries |
| HP LTO-5 Full-height with 8Gb/s Fibre Channel | AQ273F #900 | I3AZ | For use in Quantum automation tape libraries |
| HP LTO-5 Half-height with 6Gb/s SAS | AQ283B #103 | Z39W | For use in HP MSL G3 tape libraries |

With all four 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.

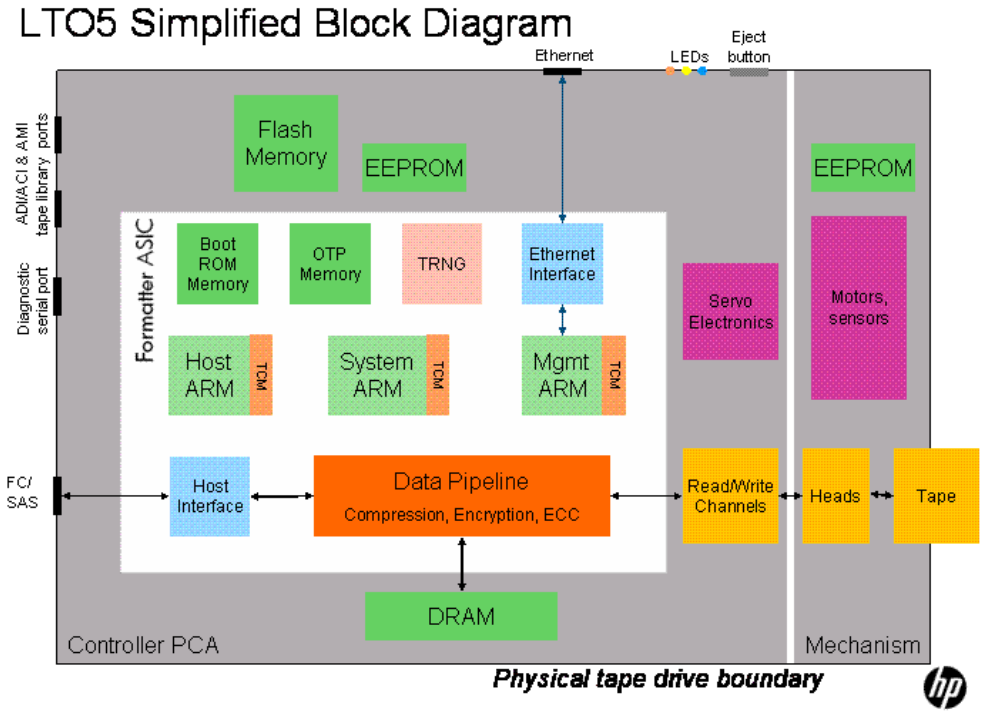



**Figure 2 Hardware Block Diagram**

## 3 FIPS 140-2 Security Level

The HP LTO-5 meets the security requirements established in FIPS 140-2 for an overall module security of Level 1 with the individual requirements and corresponding security level detailed in Table 1.

| FIPS 140-2 Security Requirement Area | 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 | N/A |
| Cryptographic Key Management | 1 |
| Electromagnetic Interference / Electromagnetic Compatibility | 1 |
| Self-Tests | 1 |
| Design Assurance | 1 |
| Mitigation of Other Attacks | N/A |

**Table 1 HP LTO-5 Security Levels**

# 4 Cryptographic module ports and interfaces

There are two different host interfaces for data transfer, both of which implement an ANSI standard interface:

i) Fibre Channel
ii) SAS.

Fibre Channel drives are equipped with up to two SFP duplex-LC short-wave 8 Gb/s fibre connectors. The drives are capable of switched fabric attach, public loop or private loop and operate at 8 Gb/s, 4 Gb/s or 2 Gb/s after auto-speed negotiation.

SAS drives are equipped with a standard internal SAS connector.

In addition to the host interface port, there are three serial ports and an Ethernet port for device manageability:

- The diagnostics serial port on the back of the drive,
- The AMI (Automation Management Interface) serial port on the back of the drive,
- The larger ACI/ADI (Automation Communications/Drive Interface) connector on the back of the drive.
- The iADT (Ethernet) port is available for key management communications.

The module has a slot and spring loaded cover through which a tape is inserted.

The host interface supports the SCSI command protocol. If a module is to be used in a tape library, the library controls the module using the Automation Controller Interface.

There is an eject button at the top-right of the module front panel. This is used to manually eject a tape.

There is a reset switch that is accessed through a pin-hole immediately below the right hand end of the eject button.

There are five LED indicators immediately below the eject button. They are from top to bottom: “Ready”, “Drive Error”, “Tape Error” “Clean” and “Encryption”.

Power for the HP LTO-5 Fibre Channel Tape Drive is supplied to the module through a standard 4-pin power connector used to supply the 5V and 12V power the tape drive requires. Power for the HP LTO-5 SAS Tape Drive is provided through an industry standard SAS connector.

| Interface | Description | Types of data processed by interface |
|---|---|---|
| Data input | Host interface | Plaintext data to encrypt and store on tape. Specific SCSI command to set (plaintext) cryptographic key. |
| | Tape read heads | Encrypted data is read from the |

| | | |
|---|---|---|
| | | tape into the module to be decrypted and passed to the host interface. |
| Data output | Host interface | Plaintext data that has been read from tape and decrypted. |
| | Tape write heads | Host data is encrypted and written to tape. |
| Control input | Host Interface, Autoloader management interface. | SCSI commands. Specific SCSI command to set cryptographic key. |
| | Ethernet port | TLS-secured protocol via Ethernet port to establish a Key Encrypting Key. |
| Status output | Host Interface, Front panel LEDs, Ethernet port | Output data generated by SCSI commands, module status |

**Table 2 HP LTO-5 Ports and Interfaces**

# 5 Roles, Services, and Authentication

## *5.1 Roles and Services*

The HP LTO-5 meets all FIPS 140-2 level 1 requirements for Roles and Services, implementing both a Crypto-Officer role and a User role. As the HP LTO-5 is a level 1 module, role-based authentication is not supported. An operator implicitly assumes the role of either Crypto-Officer or User by selecting a service associated with that role.

The following table, Table 3, summarizes the services available to each role.

| Role | Purpose | Services |
|---|---|---|
| Crypto Officer | Module configuration | • Set and get security parameters<br>• Upgrade module firmware<br>• Zeroize |
| User | Usage of module functionality | • Write data to tape<br>• Read data from tape<br>• Reserve<br>• Release<br>• Load/Unload<br>• Verify tape data<br>• Erase tape data<br>• Tape control and configuration commands<br>• Report commands<br>• Status commands<br>• Logging commands |

**Table 3 Summary of Roles and Services**

The User role is assumed when an operator accesses a User service. Similarly, the Crypto-Officer role is assumed when an operator accesses a Crypto-Officer service.

### *5.2 Access to Services*

Although there is no role-based authentication in the module, in case of the firmware upgrade service, the firmware upgrade image is digitally signed using RSA. Before the upgrade can occur, the signature is verified by the module firmware. If the actual signature does not match the value calculated by the module, then the upgrade is not allowed.

* Note: If a non-FIPS validated firmware version is loaded onto the module, then the module is no longer a FIPS validated module.

Access to the majority of the services of the module is via SCSI commands. Each service corresponds to one or more SCSI commands.

The following table, Table 4, lists the authorized services linked to each of the Roles offered by the module.

| Role | Authorized Services | SCSI commands |
|---|---|---|
| User | Write data to tape | WRITE<br>WRITE ATTRIBUTE<br>WRITE FILEMARKS |
| | Read data from tape | READ<br>READ ATTRIBUTE |
| | Reserve | RESERVE<br>PERSISTENT RESERVE IN<br>PERSISTENT RESERVE OUT |
| | Release | RELEASE<br>PERSISTENT RESERVE IN<br>PERSISTENT RESERVE OUT |
| | Load/Unload | LOAD/UNLOAD |
| | Verify tape data | VERIFY |
| | Erase tape data | ERASE |
| | Tape control and configuration commands | FORMAT MEDIUM<br>LOCATE<br>MODE SELECT<br>MODE SENSE<br>PREVENT/ALLOW MEDIUM REMOVAL<br>REQUEST SENSE<br>REWIND<br>SET CAPACITY<br>SET DEVICE IDENTIFIER<br>SET TIMESTAMP<br>SETUP IP CONFIGURATION<br>SPACE<br>WRITE BUFFER |
| | Report commands | MAINTENANCE IN/OUT<br>READ BLOCK LIMITS |

| Role | Authorized Services | SCSI commands |
|---|---|---|
| | | READ BUFFER<br>READ LOGGED-IN HOST TABLE<br>READ MEDIA SERIAL NUMBER<br>READ POSITION<br>REPORT DENSITY SUPPORT<br>REPORT DEVICE IDENTIFIER<br>REPORT IP CONFIGURATION<br>REPORT LUNS<br>REPORT SUPPORTED OPCODES<br>REPORT SUPPORTED TASK MANAGEMENT FUNCTIONS<br>REPORT TARGET PORT GROUPS<br>REPORT TIMESTAMP |
| | Status commands | INQUIRY<br>RECEIVE DIAGNOSTICS RESULTS<br>SEND DIAGNOSTIC<br>TEST UNIT READY |
| | Logging commands | LOG SELECT<br>LOG SENSE |
| Crypto Officer | Upgrade module firmware | Enhanced FIRMWARE UPGRADE<br>DOWNLOAD FIRMWARE SEGMENT<br>Enhanced FIRMWARE UPGRADE REBOOT<br>Enhanced FIRMWARE UPGRADE REPORT IMAGE INFO |
| | Set and get security parameters | SECURITY PROTOCOL IN<br>SECURITY PROTOCOL OUT |
| | Zeroize | This is not a SCSI command. All CSPs are actively overwritten with zeroes. |

**Table 4 Services Authorized for Roles**

# 6 Secure Operation and Rules

## *6.1 Security Rules*

In order to operate the HP LTO-5 product in a FIPS Approved mode, 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.

# 7 Access Control Policy

Much of the module access control policy has already been covered in earlier sections of this document. This section deals explicitly with Cryptographic Keys and CSPs.

## *7.1 Cryptographic Keys and CSPs*

The module uses a number of keys for data encryption, integrity checking and authentication. Table 5 lists all keys.

| Key | Purpose | Generation | Key input | Key output | Key storage | Key Zeroization |
|---|---|---|---|---|---|---|
| **Root CA public key (RTPK)** | Forms the basis of the "trust tree". 2048 bit RSA public key. Used to authenticate Transport Layer Security (TLS) connection between host and module. | Externally generated | Installed during the drive commissioning process | N/A | EEPROM. Has a Message Authentication Code (using the Root key) to verify it's integrity | This is a public key and so key zeroization is not required. |
| **Management Host public key (MHPK)** | A trusted Host public key. This is a 2048-bit RSA key. Used to authenticate management host to drive to permit installing and deleting certificates and changing secure mode. | Externally generated | Drive commissioning process | N/A | RAM | This is a public key and so key zeroization is not required. |
| **Drive private key (DRPV)** | A 2048 bit RSA private key used to authenticate Transport Layer Security (TLS) connection between host and module. | Externally generated | Input as part of the manufacturing process | N/A | EEPROM | This is zeroed using a Maintenance Out command. |
| **Drive public key (DRPK)** | A 2048 bit RSA public key used to authenticate Transport Layer Security (TLS) connection between host and module. | Externally generated | Input as part of the manufacturing process. | N/A | EEPROM | This is a public key and so key zeroization is not required. |
| **Key Encryption Key (KEK)** | An AES-256 key used to encrypt the data encryption key. | This key is provided by the backup application running on the host computer system. | Passed encrypted within a TLS session across the Ethernet interface or supplied in plaintext across host interface (FC or SAS) in a direct point-to-point configuration. | N/A | RAM | The Key Encryption Key is zeroed at power up, so power cycling the drive will zero the key. |
| **TLS Pre-Master Secret (TLSP)** | Used by TLS to establish the session keys. | During TLS session establishment | Generated internally so N/A | N/A | Stored in RAM only for duration of the TLS session | The TLS pre-master key is zeroized after the TLS session is closed. |

| Key | Purpose | Generation | Key input | Key output | Key storage | Key Zeroization |
|---|---|---|---|---|---|---|
| **TLS HMAC Key (TLSH)** | TLS HMAC Key to provide data integrity over TLS session. | During TLS session establishment | Generated internally so N/A | N/A | Stored in RAM only for duration of the TLS session | The TLS HMAC key is zeroized after the TLS session is closed. |
| **TLS Encryption Key (TLSK)** | An AES-128 or AES-256 key used provide data protection over TLS session. | During TLS session establishment | Generated internally so N/A | N/A | Stored in RAM only for the duration of the TLS session | The TLS Encryption key is zeroized after the TLS session is closed. |
| **Data Encryption Key (DEK)** | An AES-128 or AES-256 key used to encrypt data written to tape and decrypt data read from tape. | FIPS compliant RNG | Internally generated, so N/A. | N/A | Stored in the RAM while used to encrypt or decrypt data and stored on the tape in encrypted form, encrypted by the Key Encryption Key using AES key wrapping. | This is stored on the tape as an encrypted key and so key zeroization is not required. If zeroization is required while key is in the System ARM, the Data Encryption Keys are zeroed at power up, so power cycling the drive will zero the key. |
| **Firmware OTP public key, also known as "HP public key" (HPPK)** | An 2048-bit RSA public key used to check signature of boot loader firmware at startup. | Externally generated | Written to OTP during manufacture | N/A | OTP | This is a public key and so key zeroization is not required. |

| Key | Purpose | Generation | Key input | Key output | Key storage | Key Zeroization |
|---|---|---|---|---|---|---|
| **Firmware public key (IPK)** | An 2048-bit RSA public key used to authenticate firmware upgrades by checking the signature on any new firmware image before installing it. | Externally generated | Firmware build process | N/A | Flash memory | This is a public key and so key zeroization is not required. |
| **Seed and Seed Key (S/SK)** | Used to initialize the Approved RNG. | Generated internally via the non-Approved RNG. | N/A | N/A | EEPROM | The Seed and Seed Key are zeroed at power up, so power cycling the drive will zero the keys. |

**Table 5 Keys used by the HP LTO-5**

### *7.1.1 Key generation*

The HP LTO-5 generates the Root key during manufacture using the on-chip “True Random Number Generator”; and the Data Encryption Key using a FIPS-compliant RNG. The Key Encryption Key is generated by the host backup application using methods beyond the scope of the tape drive.

### *7.1.2 Key entry and output*

The Firmware Public Key is built into the firmware image when it is compiled. The Key Encryption Keys are entered either in plaintext across the host interface in a point-to-point configuration, or in an encrypted form across the Ethernet port within a secure TLS session. Key entry and output for all key material is detailed in Table 5.

### *7.1.3 Key storage*

Data encryption keys are stored in the System ASIC. They are written into tightly coupled memory using write only registers and kept there until explicitly no longer required. The firmware has been written in such a way that there is no read access to these registers and memory from outside the module, either directly or through diagnostic commands. Key storage for all keys is detailed in Table 5.

### *7.1.4 Zeroization of key material*

Data encryption keys and Key Encryption Keys that are stored in memory are zeroed at power up. The Root key cannot be zeroed.

### *7.1.5 Access to key material*

The following matrices (Tables 6 and Table 7) show the access that an operator has to specific keys or other critical security parameters when performing each of the services relevant to his/her role.

| Keys / Service | RTPK | MHPK | DRPK | DRPV | KEK | TLSP | TLSH | TLSK | DEK | HPPK | IPK | S/SK |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Write data to tape | | | | | E | | | | E | | | |
| Read data from tape | | | | | E | | | | E | | | |
| Reserve | | | | | | | | | | | | |
| Release | | | | | | | | | | | | |
| Load/Unload | | | | | | | | | | | | |
| Verify tape data | | | | | E | | | | E | | | |
| Erase tape data | | | | | | | | | | | | |
| Tape control and configuration commands | | | | | | | | | | | | |
| Report commands | | | | | | | | | | | | |
| Status commands | | | | | | | | | | | | |
| Logging commands | | | | | | | | | | | | |

**Table 6 User Role**

| Keys / Service | RTPK | MHPK | DRPK | DRPV | KEK | TLSP | TLSH | TLSK | DEK | HPPK | IPK | S/SK |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Upgrade module firmware | | D | | | D | D | D | D | D | | E | |
| Set and get security parameters | | W | W | W | W | W | W | W | W | | | W |
| Zeroize | | D | D | D | D | D | D | D | D | | | D |

**Table 7 Crypto-Officer Role**

**Type of access required to key**

blank None
W Write access
R Read Access
D Delete Access
E Execute Access

Keys

| | |
|---|---|
| RTPK | Root CA Public Key |
| MHPK | Management Host Certificate Public Key |
| DRPK | Drive Public Key |
| DRPV | Drive Private Key |
| KEK | Key Encryption Key |
| TLSP | TLS Pre-Master Secret |
| TLSH | TLS HMAC Key |
| TLSK | TLS Encryption Key |
| DEK | Data Encryption key |
| HPPK | Firmware OTP public key, also known as “HP Public Key” |
| IPK | Firmware Public Key |
| S/SK | Seed and Seed Key |

## *7.2 Public Key Certificates*

| Key | Purpose | Generation | Key input | Key output | Key storage | Key Zeroization |
|---|---|---|---|---|---|---|
| **Root CA Certificate** | Forms the basis of the “trust tree”. | Externally generated | Installed during drive commissioning process | N/A | EEPROM. Has a Message Authenticatio n Code (using the Root key) over it to verify it’s integrity | This only contains public key material and so key zeroization is not required. |
| **Drive Certificate** | Authenticates the Drive to a Management Host or key manager | Externally generated | Drive manufacturing process | N/A | EEPROM | This only contains public key material and so key zeroization is not required. |
| **Management Host certificate** | Authenticates the management host to the Drive. | Externally generated | Supplied by the management host | N/A | RAM | This only contains public key material and so key zeroization is not required. |
| **Key Manager Certificate** | Authenticates the Key Manager to the Drive | Externally generated | Supplied by the Key Manager | N/A | RAM | This only contains public key material and so key zeroization is not required. |

**Table 8 Certificates Used Within the HP LTO-5**

# 8 FIPS-Approved algorithms

The module uses the following FIPS Approved algorithms:

- AES (256-bits ECB, CTR modes) to encrypt host data and EEPROM contents (Cert. #1441)
- AES GCM (Cert. #1441)
- ANSI X9.31 RNG (w/AES 256) (Cert. #790)
- AES (256-bit ECB mode) (Cert. #1442)
- RSA (2048-bit verify) to authenticate a firmware upgrade prior to upgrading the firmware (Cert. #708)
- SHA-256 (Cert. #1308)
- AES (128-bit and 256-bit, CBC mode) (Cert. #1443)
- AES GCM (Cert. #1444)
- RSA (2048-bit sign/verify) (Cert. #709)
- SHA-1, -224, -256, -384, -512 (Cert. #1309)
- HMAC (w/SHA-1, -224, -256, -384, -512) (Cert. #848)
- ANSI X9.31 RNG (w/AES 128, 192, 256) (Cert. #791)

The TLS connection is then used to encrypt and transfer a Key Encryption Key.
The approved mode uses the TLS_RSA_WITH_AES_256_CBC_SHA and TLS_RSA_WITH_AES_128_CBC_SHA ciphersuites. The ciphersuite to use in a key exchange is negotiated as part of that protocol. If there are attempts to use an unsupported or unapproved TLS ciphersuite, then the module rejects it. This behavior occurs when the relevant certificates are installed, as required for FIPS mode (see section 11, item 6).

# 9 Non-FIPS Approved but Allowed Algorithms

The module implements the following non-Approved, but allowed algorithms:

- AES Key Wrap as per the NIST recommended Key Wrap Specification (AES Cert. #1441, key wrapping; key establishment methodology provides 256 bits of encryption strength)
- The module implements a non-Approved RNG for seeding the ANSI X9.31 RNG
- MD5 is used in TLS establishment in accordance with FIPS140-2 Implementation Guidance, which is allowed for use in FIPS mode.

# 10 Non-Approved modes of operation

The HP LTO-5 contains a TLS implementation.
One TLS mode, using the TLS_DH_anon_AES_256_CBC_SHA ciphersuite, is anonymous. Use of this mode of TLS will result in operating the cryptographic module outside of FIPS mode.

# 11 FIPS mode

In order to be FIPS 140-2 compliant, the module must be operated according to a set of security procedures. When used in this way, the module is operating in its FIPS mode of operation. FIPS mode is defined as follows:

1. The product is assumed to be operating in a physically secure environment
2. The product's host application is assumed to be operating in a physically secure environment
3. The Root CA is installed in a physically secure environment
4. The product is operated exclusively as an encrypting tape drive. In order to operate in "FIPS mode", all host applications will only store encrypted data.
5. If plaintext Key Encryption Keys are used, the connection between the host application and the HP LTO-5 must be physically secure.
6. If a TLS connection is used to transfer Key Encryption Keys, the relevant certificates must be installed to enable authentication to be performed.

# 12 Self-Tests

The HP LTO-5 implements both power-up and conditional self tests as required by FIPS 140-2. The following two sections outline the tests that are performed.

## *12.1 Power-up self-tests*

Each of these tests is executed when the module is turned on and the module first executes. If any of these tests fail, the module will not load. The module must be reset to re-execute these tests.

The module performs the following self-tests:

A. Cryptographic Algorithm Tests
    a. AES Encrypt/Decrypt KAT
    b. AES GCM KAT
    c. ANSI X9.31 RNG KAT
    d. AES Decrypt KAT
    e. RSA Verify KAT
    f. SHA-256 KAT
    g. AES Encrypt/Decrypt KAT
    h. AES GCM KAT
    i. RSA Sign/Verify KAT
    j. SHA-1, -224, -256, -384, -512 KAT
    k. HMAC (w/ SHA-1, -224, -256, -384, -512) KAT
    l. ANSI X9.31 KAT
B. Firmware Integrity Test: RSA Signature Verification
C. Critical Function: Drive Certificate Integrity Test

The module performs the following Conditional self-tests:

A. Continuous RNG test for both Approved and non-Approved RNGs
B. Firmware Load Test: RSA Signature Verification

If any of the above self-tests fail, the module will enter an error state indicated by a flashing Driver Error LED. The only actions possible in this state are to reset the module (which will repeat the self-tests), or load new firmware.

## 13 Design Assurance

HP employ industry standard best practices in the design, development, production and maintenance of the HP LTO-5 product, including the FIPS 140-2 module.

This includes the use of an industry standard configuration management system that is operated in accordance with the requirements of FIPS 140-2, such that each configuration item that forms part of the module is stored with a label corresponding to the version of the module and that the module and all of its associated documentation can be regenerated from the configuration management system with reference to the relevant version number.

Design documentation for the module is maintained to provide clear and consistent information within the document hierarchy to enable transparent traceability between corresponding areas throughout the document hierarchy, for instance to correspondence between elements of this Cryptographic Mode Security Policy (CMSP) and the design documentation.

Guidance appropriate to an operator's Role is provided with the module and provides all of the necessary assistance to enable the secure operation of the module by an operator, including the Approved security functions of the module.

## 14 Physical Security

The HP LTO-5 is composed of production grade components, which do not require any maintenance or inspection by the user to ensure security.

## 15 Mitigation of Other Attacks

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