Oracle StorageTek T10000C Tape Drive

Hardware Part #: 7054185

Firmware Version: 1.57.308

FIPS 140-2 Non-Proprietary Security Policy

Level 1 Validation
Version 1.0

1/21/2014

Table of Contents

List of Figures

List of Tables

INTRODUCTION

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the StorageTek T10000C Tape Drive from Oracle Corporation. This Security Policy describes how the StorageTek T10000C Tape Drive meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S. and Canadian Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) and the Communications Security Establishment Canada (CSEC) Cryptographic Module Validation Program (CMVP) website at http://csrc.nist.gov/groups/STM/cmvp.

This document also describes how to run the module in a secure FIPS-Approved mode of operation. This policy was prepared as part of the Level 1 FIPS 140-2 validation of the module. The StorageTek T10000C Tape Drive may also be referred to in this document as the Encrypting Tape Drive, the ETD[1], the crypto module, or the module.

1.2 References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The Oracle Corporation website (http://www.oracle.com) contains information on the full line of products from Oracle.

- The CMVP website (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm) contains contact information for individuals to answer technical or sales-related questions for the module.

1.3 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
- Finite State Machine
- Other supporting documentation as additional references

[1] ETD – Encrypting Tape Drive

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to Oracle. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Submission Package is proprietary to Oracle and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Oracle.

2 STORAGETEK T10000C TAPE DRIVE

2.1 Module Overview

The StorageTek T10000C Tape Drive by Oracle Corporation (Hardware Part #: 7054185; Firmware Version: 1.57.308) blends the highest capacity, performance, reliability, and data security to support demanding, 24/7 data center operations. The StorageTek T10000C Tape Drive ("Encrypting Tape Drive" or ETD) delivers the world's fastest write speeds (252 MB[2]/sec[3]) to a native five (5) Terabytes of magnetic tape storage; making it ideal for data center operations with growing data volume. The StorageTek T10000C Tape Drive provides data protection with built-in AES[4] hardware encryption.

The StorageTek T10000C Tape Drive provides Oracle customers with three different FIPS-Approved modes of operation. Customers can be assured that their data will always be secure, in any of these Approved modes. The ETD drive operates with data encryption services:

- permanently enabled
- temporarily enabled
- temporarily disabled

Each encryption mode provides FIPS 140-2 Approved security services and functionality to ETD operators. For added flexibility, a non-FIPS-Approved mode is also available.

Views from all sides of the StorageTek T10000C Tape Drive are provided as Figure 1 through Figure 6.

[2] MB – Megabytes
[3] sec – Second
[4] AES – Advanced Encryption Standard

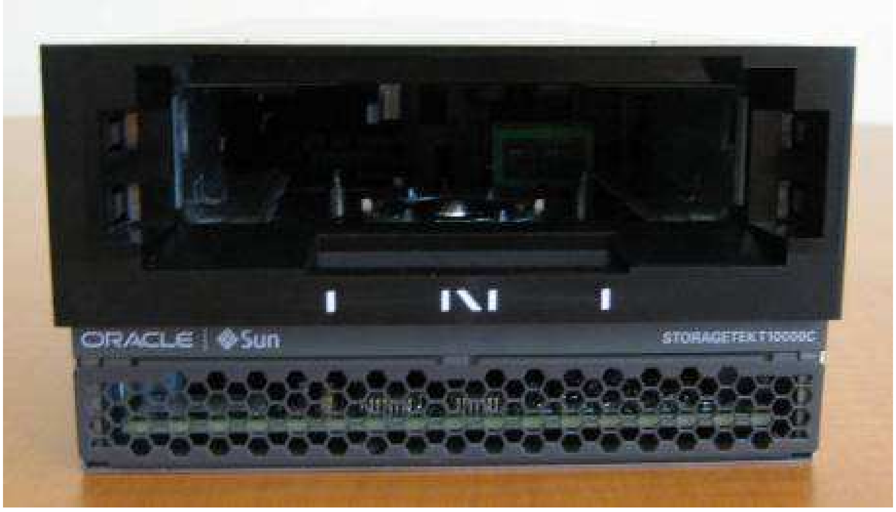

Figure 1 – StorageTek T10000C Tape Drive (Front)

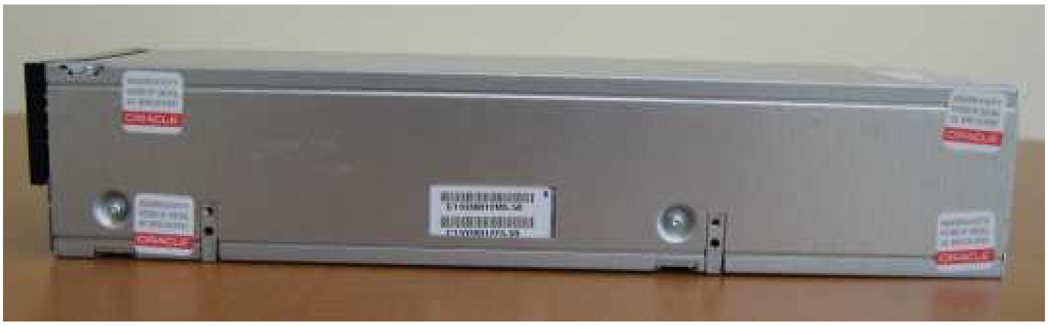

Figure 2 – StorageTek T10000C Tape Drive (Right Side)[5]

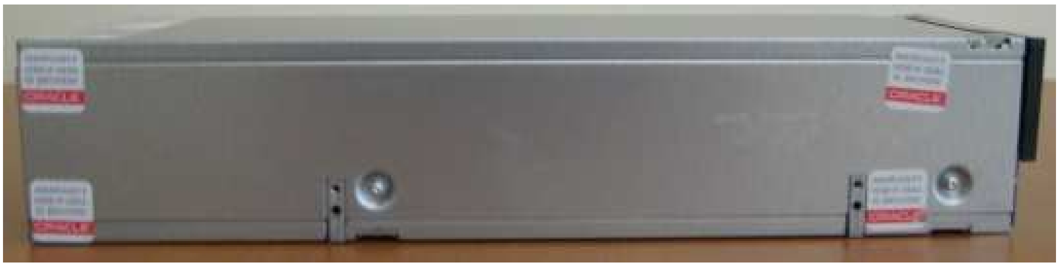

Figure 3 – StorageTek T10000C Tape Drive (Left Side) [6]

[5] The labels shown in the figure do not provide additional physical security

[6] The labels shown in the figure do not provide additional physical security

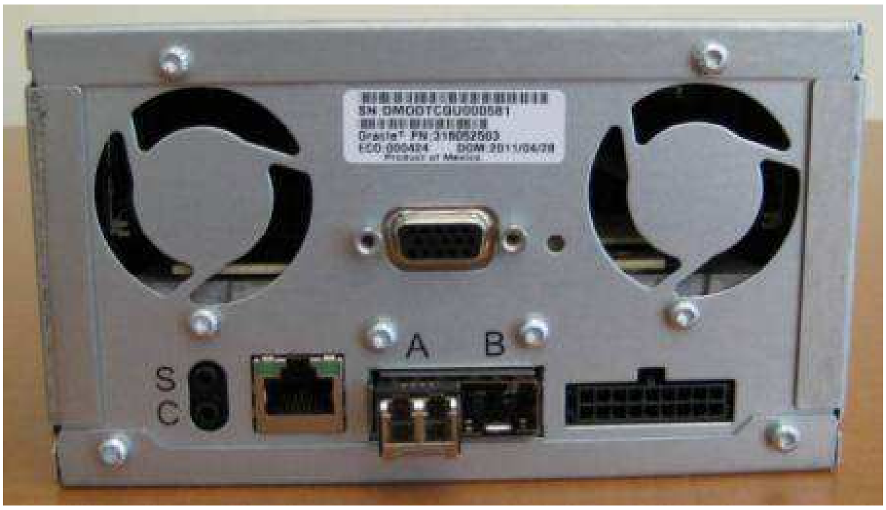

Figure 4 – StorageTek T10000C Tape Drive (Rear)

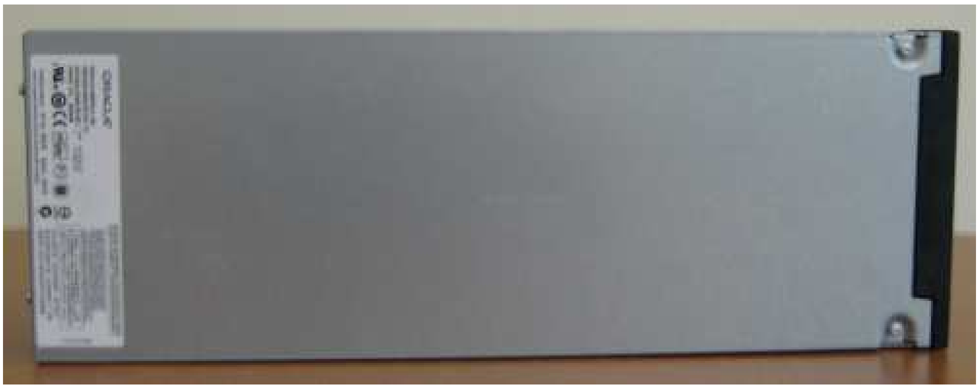

Figure 5 – StorageTek T10000C Tape Drive (Top)

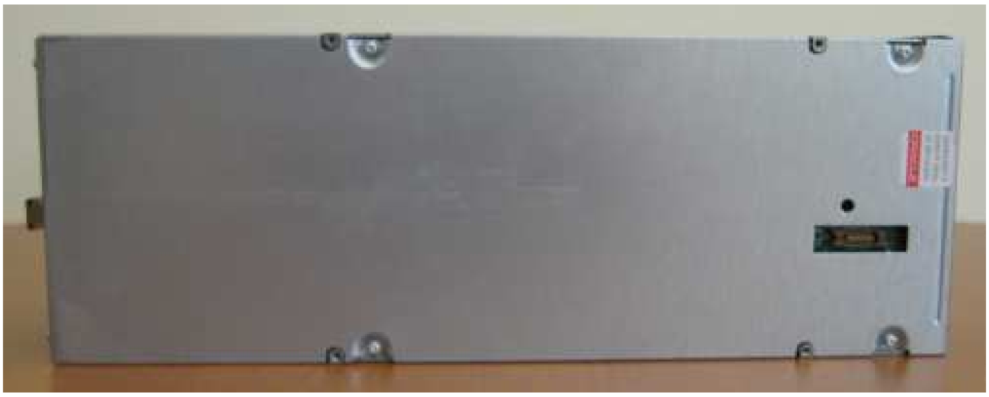

Figure 6 – StorageTek T10000C Tape Drive (Bottom) [7]

[7] The label shown in the figure does not provide additional physical security

2.1.1 Oracle Key Manager

The ETD is intended to be used in conjunction with the Oracle Key Manager (OKM), which provides centralized key management. The OKM, an external system component, creates, stores, and manages the keys used for encryption and decryption of data stored in the tape cartridge used by the ETD. An Oracle Key Manager (formerly called the Key Management System or KMS) cluster consists of two or more Key Management Appliances (KMAs), providing policy-based Lifecycle Key Management, authentication, access control, and key provisioning services. Connections to the ETD from the OKM are secured through the use of TLS[8] 1.0[9].

2.1.2 Virtual Operator Panel

The Virtual Operator Panel (VOP) is an external software application running on a General Purpose Computer (GPC) that facilitates operator communication with the StorageTek T10000C Tape Drive through the use of an intuitive and user-friendly Graphical User Interface (GUI). The VOP allows an operator to configure the drive for FIPS-Approved operation, perform operator services, and display drive-related status information. An operator of the StorageTek T10000C Tape Drive will use the VOP, in addition to the OKM, during the initial FIPS configuration and any time the operator chooses to switch between FIPS-Approved modes. Connections to the ETD from the VOP are provided through the Telnet network protocol.

2.1.3 StorageTek T10000C Tape Drive Deployment

A sample deployment scenario for the StorageTek T10000C Tape Drive with encryption enabled is provided in Figure 7 below. The ETD is shown with a red, dotted line surrounding it, representing its cryptographic boundary.

[8] TLS – Transport Layer Security

[9] The TLS 1.0 protocol has not been reviewed or tested by the CAVP and CMVP.

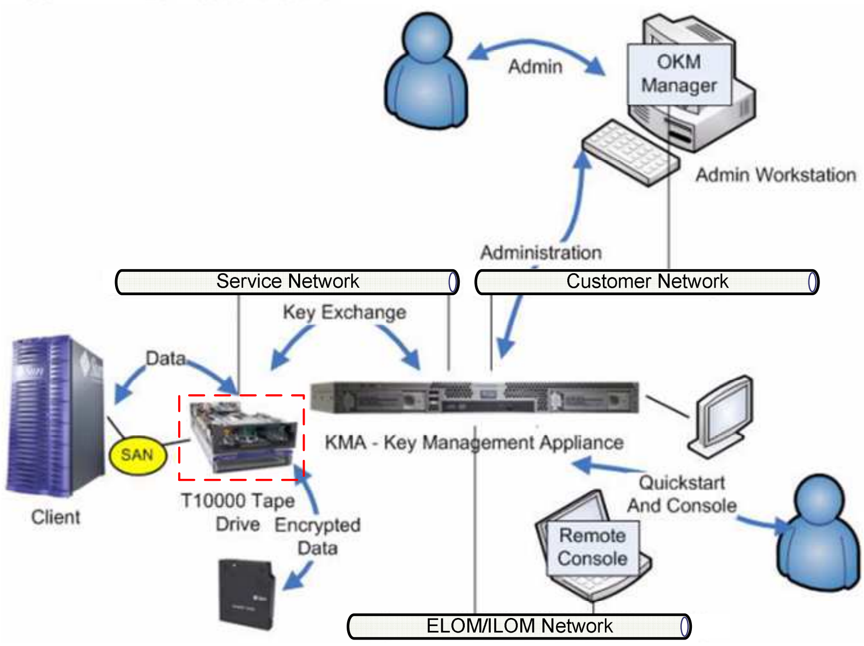

Figure 7 – StorageTek T10000C Tape Drive Deployment Scenario

2.2 Module Specification

The StorageTek T10000C Tape Drive is validated at the FIPS 140-2 section levels shown in Table 1 for all three FIPS-Approved modes of operation.

Table 1 – Security Level per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	1
4	Finite State Model	1
5	Physical Security	1
6	Operational Environment	N/A
7	Cryptographic Key Management	1
8	EMI/EMC[10]	1
9	Self-tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A

[10] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility

The StorageTek T10000C Tape Drive is a hardware cryptographic module with a multi-chip standalone physical embodiment as defined by FIPS 140-2. The primary purpose of this device is to provide FIPS 140-2 Level 1 security to data being stored on magnetic tape. The cryptographic boundary of the StorageTek T10000C Tape Drive is defined by the tape drive's commercial-grade, metallic enclosure.

The module provides three FIPS-Approved modes of operation that each meet overall Level 1 FIPS 140-2 requirements specified in Table 1 above. The module also provides one non-FIPS-Approved, or non-Approved, mode of operation. Each of the Approved modes and the non-Approved mode are described in the sections below. Cryptographic security functions and services available in each of the defined modes are specified in the appropriate sections of this Security Policy. Additional information on each operational mode of the module, including their invocation, is provided in Section 3 (Secure Operation).

2.2.1 Permanent Encryption Approved Mode

The Permanent Encryption Approved Mode or Permanent Encryption Mode is the first FIPS-Approved mode of operation provided by the StorageTek T10000C Tape Drive. This mode provides secure encryption and decryption of data stored on magnetic tape, using the 256-bit AES cryptographic algorithm. While operating in the Permanent Encryption Mode, operators of the module do not have the ability to disable encryption services. Placing the module into Permanent Encryption Mode is non-reversible. The ETD will be able to read from unencrypted tape cartridges while operating in this mode, but will be unable to append to them if unencrypted data is already present.

To determine that the module is operating in the Permanent Encryption Mode, an operator can use the VOP to view the drive settings and verify that the "Encryption Active" and "Permanently encrypting" labels are both set to "Yes". The operator can also check that the Encryption Status LED[11] on the back of the module is a solid red color. In addition, the operator shall verify that the "Use KMS or DPKM[12]" label is set to "KMS". Instructions to place the module into the Permanent Encryption Mode are provided in Section 3.1.4 (Permanent Encryption Approved Mode Set-Up).

2.2.2 Encryption Enabled Approved Mode

The second FIPS-Approved mode of operation is the Encryption Enabled Approved Mode or Encryption Enabled Mode. The Encryption Enabled Mode provides operators the ability to encrypt and decrypt data that is stored on a magnetic tape source. Encryption and decryption are performed using the 256-bit

[11] LED – Light Emitting Diode
[12] DPKM – Data Path Key Management

AES cryptographic algorithm. This mode operates in the same way as the Permanent Encryption Mode, but with the ability to switch to the Permanent Encryption, the Encryption Disabled Approved modes and the non-Approved mode. The ETD will be able to read from unencrypted tape cartridges while operating in this mode, but it will be unable to append to them if unencrypted data is already present.

An operator of the module can determine if the module is operating in the Encryption Enabled Mode by using the VOP to view the drive settings and verify that the "Encryption Active" label is set to "Yes" and the "Permanently encrypting" label is set to "No". The operator can also check that the Encryption Status LED on the back of the module is a solid red color. Finally, the operator shall confirm that the "Use KMS or DPKM" label is set to "KMS". Instructions to place the module into the Encryption Enabled Mode are provided in Section 3.1.3 (Encryption Enabled Approved Mode Set-Up).

2.2.3 Encryption Disabled Approved Mode

The Encryption Disabled Approved Mode or Encryption Disabled Mode is the last FIPS-Approved mode. When operating in the Encryption Disabled Mode, only plaintext data is stored on the magnetic tape. This plaintext data is non-security-relevant user data. While operating in this mode, only unencrypted tape cartridges will be supported for read and write operations. An operator will be able to switch to any of the additional FIPS-Approved modes or the non-Approved mode while operating the module in the Encryption Disabled Mode.

An operator of the module can determine if the module is operating in the Encryption Disabled Mode by using the VOP to view the drive settings and verify that the "Encryption Active" label is set to "No". The operator can also confirm that the Encryption Status LED on the back of the module is a solid green color. Finally, the operator shall confirm that the "Use KMS or DPKM" label is set to "UNKN[13]". Instructions to place the module into the Encryption Disabled Mode are provided in Section 3.1.2 (Encryption Disabled Approved Mode Set-Up).

2.2.4 non-FIPS-Approved Mode

The StorageTek T10000C Tape Drive is capable of operating in a non-FIPS-Approved Mode or non-Approved mode of operation. The module is defined as operating in the non-Approved mode when DPKM is enabled through the VOP. DPKM allows an operator to use the SCSI[14]4 commands `SPIN` and `SPOUT` in order to import and export keying material to and from the module in plaintext. While operating in the non-Approved mode, the drive is still capable of operating with encryption services enabled or disabled. The ETD is also capable of

[13] UNKN - Unknown

[14] SCSI – Small Computer System Interface

switching back-and-forth between encryption services[15] disabled (non-compliant) and encryption services enabled (non-compliant) at will; without the use of a bypass test.

Keys and CSPs established in any of the three Approved modes are zeroized prior to operating in the non-Approved mode. The operator is not able to update the firmware while operating in this mode. An operator of the module can determine if the module is operating in the non-Approved mode by using the VOP to confirm that the "Use KMS or DPKM" label is set to "DPKM". Instructions to place the module into the non-Approved mode are provided in Section 3.3 (Cryptographic Officer Guidance (Non-Approved Mode)).

2.3 Module Interfaces

The following is a list of the FIPS 140-2 logical interfaces supported by the StorageTek T10000C Tape Drive:

- Data Input
- Data Output
- Control Input
- Status Output

Additionally, the module supports a Power Input interface.

2.3.1 FIPS 140-2 Logical Interface Mapping

Figure 1 in Section 2.1 (Module Overview) shows the front of the StorageTek T10000C Tape Drive. The opening provides an entryway for an approved StorageTek T10000C Tape Cartridge. The ETD will not operate if the wrong tape cartridge is inserted. This entryway provides the Tape Head and RFID[16] Reader/Writer as physical interfaces to the tape cartridge. The opening at the front of the module is the only opening in the module. It does not provide access to the interior of the module.

Figure 4 in Section 2.1 (Module Overview) shows the rear of the StorageTek T10000C Tape Drive. It provides the following physical interfaces:

- Tape Transport Interface (TTI) – RS-232[17] connection
- Power Supply Connector
- Host Interfaces – Fibre Channel connection
- Recessed Switch
- Ethernet Port – RJ45[18] connection

[15] Non-compliant encryption performed in the non-FIPS-Approved Mode can also be referred to as "obfuscation". The output from this service is equivalent to plaintext.
[16] RFID – Radio Frequency Identification
[17] RS-232 – Recommended Standard 232

- Encryption Status LED
- Drive Status LED

The bottom of the StorageTek T10000C Tape Drive (Section 2.1, Figure 6) provides one additional physical interface; the Operator Panel Port. This port is used to provide general module status as well as additional control input access when the drive is rack-mounted.

Table 2 provides a mapping of all of the physical interfaces of the StorageTek T10000C Tape Drive listed above to their respective FIPS 140-2 Logical Interfaces. The functionality and logical interface mappings of these physical interfaces do not change between Approved modes.

Table 2 – Mapping of FIPS 140-2 Logical Interfaces to StorageTek T10000C Tape Drive Physical Interfaces

Physical Interface	Quantity	FIPS 140-2 Logical Interfaces Supported	Description
Tape Head	2	Data Input Data Output	Provides the interface to the magnetic tape media, where the user data to be encrypted is written to, and where the data to be decrypted is read from. Tape media resides in six possible cartridge types: 1) Standard Data 2) SPORT (reduced length) Data 3) VolSafe (write-once) Data 4) Sport VolSafe Data (reduced length, write-once) 5) Cleaning 6) Diagnostic (used by a service representative)
Encryption Status LED	1	Status Output	Provides status on the encryption configuration of the ETD. Additional information provided in Table 4.
TTI connector (RS232/DB15)	1	Control Input Data Output Status Output	Primarily used for tape library communications. The operator can review the status output to determine if the module has passed or failed different self-tests. The status output from this port consists of messages indicating failure and success.
Recessed switch	1	Control Input	Short press: Reset the module's IP[19] address to the default IP address (10.0.0.1) Long press: Force unencrypted ETD data dump[20]

[18] RJ45 – Registered Jack 45

[19] IP – Internet Protocol

[20] All unencrypted dumps shall be deleted by the CO after their creation

Physical Interface	Quantity	FIPS 140-2 Logical Interfaces Supported	Description
Power supply connector	1	Power	100-240 VAC[21] @ 50-60 Hz[22]
Interface Port (Host Interface)	2	Data Input Data Output Control Input Status Output	This interface is used to transfer user data between the ETD and the host. When the host transfers user data to the ETD through this interface, the ETD encrypts and writes the data to the magnetic media. When the host receives user data from the ETD through this interface, the ETD delivers data read from the magnetic media that has been decrypted by the ETD. The interface can be configured to support one of two protocols: 1) Fibre Channel, in accordance with the Fibre Channel Protocol-3 (FCP-3), SCSI Primary Commands-3, and SCSI Stream Commands (SSC-3) specifications 2) FICON[23], in accordance with the Fibre Channel Single-Byte Command Code Sets-3 Mapping Protocol (FC-SB-3), Revision 1.6 specification
Ethernet Port (RJ45)	1	Data Input Data Output Control Input Status Output	The primary uses of this interface is to: 1) Configure the ETD 2) Deliver encryption keys to the ETD 3) Obtain ETD status and diagnostic data 4) Download firmware to the ETD 5) Deliver status information to an SNMP[24] server.
Drive Status LED	1	Status Output	Provides status on the overall state of the ETD. The Tape Drive's user manual includes information regarding the different statuses that are provided by the drive through the LEDs. Additional information provided in Table 3.

[21] VAC – Volts Alternating Current
[22] Hz - Hertz
[23] FICON – Fibre connection
[24] SNMP – Simple Network Management Protocol

Physical Interface	Quantity	FIPS 140-2 Logical Interfaces Supported	Description
Operator Panel Port[25]	1	Status Output Control Input	The Bottom cover of the ETD has an Operator Panel connector carrying the following signals: A. Four signals to provide status output: 1. Power Indicator output signal 2. Activity Indicator output signal 3. Clean Indicator output signal 4. Service Indicator output signal B. An LCD[26] display output interface. The LCD is used to display ETD status and configuration menu text. C. Four switch signals (input): 1. IPL[27] Switch 2. Unload Switch 3. Menu Switch 4. Select Switch
RFID Reader/Writer	1	Data Input Data Output	Used to obtain information from each tape inserted into the ETD to reduce access times and manage the lifecycle of the cartridge. Various statistical data and information of record locations are written to the RFID located on the tape cartridge

2.3.2 StorageTek T10000C Tape Drive LED Status Information

The StorageTek T10000C Tape Drive provides two LEDs at the rear of the module which provide important status information about the module. The first LED is the Drive Status LED, which provides the overall status of the ETD. Table 3 provides a brief description of each LED state of the Drive Status LED. LEDs related to "hardware failure" or "service required" shall be reported to the Oracle StorageTek support team.

Table 3 – Drive Status LED Description

LED State	Description
Off	Drive is powered off

[25] Status and control information provided through Operator Panel Port is provided in Chapter 2 of the *StorageTek T10000 Tape Drive Operator's Guide.*

[26] LCD – Liquid Crystal Display

[27] IPL – Initial Program Load

LED State	Description
Red (Solid[28])	Hardware failure (processor error)
Red (Slow Flash[29])	Drive is starting up
Red (Fast Flash[30])	Module data dump in progress
Amber (Steady)	Service required
Amber (Slow Flash)	Functional code is loading
Amber (Fast Flash)	Firmware update in progress
Green (Solid)	Drive is operational
Green (Slow Flash)	Drive is operational (dump file present)
Green (Fast Flash)	Firmware update completed
Red/Blue (Alternating)	Hardware failure (during POST[31])
Red/Green (Alternating)	Continuous module errors; Service required

A second LED, which provides the status of the encryption configuration of the module, is the Encryption Status LED. Table 4 provides a brief description each LED state of the Encryption Status LED.

[28] LED is illuminated and not flashing
[29] Slow flash rate is one cycle per second
[30] Fast flash rate is two cycles per second
[31] POST – Power-On Self-Test

Table 4 – Encryption Status LED Description

LED State	Description
Red (Solid)	Encryption enabled/active
Red (Slow Flash)	Encryption or Decryption in progress
Amber (Solid)	Tape cartridge not present
Green (Solid)	Encryption disabled
Green (Slow Flash)	Module Reset
Red/Green/Amber (Alternating)	Module zeroed

2.3.3 StorageTek T10000C Tape Drive VOP Status Information

The module outputs status information via the Ethernet Port to the VOP to provide a more detailed drive status to the operator. Table 5 provides a brief description of the status indicators provided by the VOP.

Table 5 – VOP Status Indicators

Indicator	Color	Description
All	Black	No tape drive connection
Loaded or Unloaded	Blue	Cartridge Loaded
	Grey	Cartridge loaded in slot, not in drive
	Magenta	Cartridge loading/unloading
Empty	Grey	Cartridge not present
Online or Offline	Blue	Drive online (Indicator reads *Online*)
	Grey	Drive offline (Indicator reads *Offline*)

Indicator	Color	Description
	Magenta	Transitioning between Online/Offline
Clean	Orange	Drive needs to be cleaned
Dump	Orange	Dump present
Encryption	Red	Encryption enabled (all keys present) (Indicator reads *Armed*)
	Orange	Missing encryption key (Indicator reads *Enrolled*)
	Green	Drive not enrolled with OKM (Indicator reads *Unenrolled*)
Active or Hibernate	Blue	Hibernation activated[32]
	No color	Drive is hibernating

2.4 Roles and Services

The StorageTek T10000C Tape Drive cryptographic module provides two roles which operators may assume:

- Cryptographic Officer (CO)
- User

Each role is assumed implicitly by an operator and is determined by the service which the operator is executing. The ETD supports up to six concurrent operators. Each connection to the ETD is logically separated by the module by uniquely encrypted sessions.

Each role, and the services available to them in each Approved mode, is detailed in the sections below. Please note that the keys and Critical Security Parameters (CSPs) listed in the tables indicate the type of access required using the following notation:

- R – Read: The item is read or referenced by the service.
- W – Write: The CSP is established, generated, modified, or zeroized.

[32] This is a power-saving mode

- X – Execute: The CSP is used within an Approved or Allowed security function.

2.4.1 Crypto-Officer Role

The CO is in charge of the initial configuration of the StorageTek T10000C Tape Drive which includes placing the module into one of the three Approved Modes. A list of services available to the CO, and the Approved mode the service is available in, is provided in Table 6.

Table 6 – Cryptographic Officer Services

Service	Description	Approved Mode	CSP and Type of Access
Enable Permanent Encryption Mode	Provide public and private keys in order to connect to OKM; Enable encryption	Encryption Enabled Encryption Disabled	CA_Cert – WX TDPrivKey – W TDPubKey – W
Enable Encryption Enabled Mode	Provide public and private keys in order to connect to OKM; Enable encryption	Encryption Disabled	CA_Cert – WX TDPrivKey – W TDPubKey – W
Enable Encryption Disabled Mode	Turn encryption off; OKM services are enabled	Encryption Enabled	CA_Cert – WX TDPrivKey – W TDPubKey – W
Enable non-FIPS-Approved Mode	Bring the module into a non-Approved mode of operation	Encryption Disabled	None
Configure Module	Perform routine module configuration	Permanent Encryption Encryption Enabled Encryption Disabled	None
Place drive online/offline	Add or remove Fibre Channel connectivity to the ETD	Permanent Encryption Encryption Enabled Encryption Disabled	None
Load Firmware	Update module firmware	Permanent Encryption Encryption Enabled Encryption Disabled	FSPubKey – RX FSRootCert – X
Reset	Zeroization of all keys and CSPs	Permanent Encryption Encryption Enabled	All Keys and CSPs[33] – W
Access Module via Virtual Operator's Panel (VOP)	Log into VOP and manage the module	Permanent Encryption Encryption Enabled Encryption Disabled	None

[33] Excludes DEPubKey, FSPubKey, and FSRootCert

Service	Description	Approved Mode	CSP and Type of Access
Create Dump (Encrypted)	Create an encrypted dump file and save to EEPROM[34]	Permanent Encryption Encryption Enabled	DRBG[35] 'Key' Value – WRX DRBG 'V' Value – WRX DRBG Seed – WRX DEKey – WX DEPubKey - X
Create Dump (Unencrypted)	Create an unencrypted dump file and save to EEPROM	Permanent Encryption Encryption Enabled Encryption Disabled	None
Initial Program Load (IPL)	Reinitialize module and run self-tests	Permanent Encryption Encryption Enabled Encryption Disabled	None
View Audit Log	View, download, or delete audit log	Permanent Encryption Encryption Enabled Encryption Disabled	None
View Drive Data	Read module configuration data	Permanent Encryption Encryption Enabled Encryption Disabled	None
View Error Log	View, download, or delete error log	Permanent Encryption Encryption Enabled Encryption Disabled	None
Delete Dump	Delete the currently stored dump file	Permanent Encryption Encryption Enabled Encryption Disabled	None
Delete Perms	Deletes currently stored error messages	Permanent Encryption Encryption Enabled Encryption Disabled	None
Tape Management	Load or unload a new tape cartridge into the module	Permanent Encryption Encryption Enabled Encryption Disabled	None
Run Diagnostics	Perform a diagnostic test on the module	Permanent Encryption Encryption Enabled Encryption Disabled	None

2.4.2 User Role

The User of the StorageTek T10000C Tape Drive is the everyday user of the module. The User is responsible for importing the encryption and decryption keys when operating in one of the Approved modes with encryption enabled. Once an encryption key has been obtained, the User has the ability to encrypt and

[34] EEPROM – Electronically Erasable Programmable Read-Only Memory

[35] DRBG – Deterministic Random Bit Generator

decrypt data stored on the tape cartridge. A list of services available to the User, and the Approved mode the service is available in, is provided as Table 7.

Table 7 – User Services

Service	Description	Approved Mode	CSP and Type of Access
Encrypt Data	Encrypt data from the module to the tape cartridge	Permanent Encryption Encryption Enabled	MEKey – X
Decrypt Data	Decrypt data read from the tape cartridge	Permanent Encryption Encryption Enabled	MEKey – X
Write Plaintext Data	Write plaintext data from the module to the tape cartridge	Encryption Disabled	None
Read Plaintext Data	Read plaintext data from the tape cartridge	Permanent Encryption Encryption Enabled Encryption Disabled	None
Establish TLS[36] Session	Establish connection with OKM cluster	Permanent Encryption Encryption Enabled	DRBG ‘Key’ Value – WRX DRBG ‘V’ Value – WRX DRBG Seed – WRX TLS_PM – W TLS_MS – W TLS_EMK – W TLS_DMK – W TLS_ECK – W TLS_DCK – W CA_Cert – X TDPubKey – X TDPrivKey – X
Export AES Key Wrap Key (AKWK)	Export AKWK to the OKM cluster	Permanent Encryption Encryption Enabled	DRBG ‘Key’ Value – WRX DRBG ‘V’ Value – WRX DRBG Seed – WRX AKWK – W KWKPublicKey – X TLS_EMK – X TLS_ECK – X
Import KWKPublicKey	Import the KWKPublicKey from the OKM cluster onto the module	Permanent Encryption Encryption Enabled	KWKPublicKey – W TLS_DMK – X TLS_DCK – X
Import ME_Key	Import one or more ME_Keys onto the module from the OKM cluster	Permanent Encryption Encryption Enabled	ME_Key – W TLS_DMK – X TLS_DCK – X AKWK – X

[36] TLS – Transport Layer Security

2.4.3 Additional Operator Services

In addition to CO and User services, the module provides services to operators that are not required to assume an authorized role. These services do not modify, disclose, or substitute the keys and CSPs established in one of the Approved modes. The overall security of the module is not affected by these services.

Table 8 lists the services available to operators not required to assume an authorized role. These services are available in all three Approved modes of operation.

Table 8 – Additional Operator Services

Service	Description	Approved Mode	CSP and Type of Access
Show Status	Determine the current status of the module by reading the Encryption and Drive Status LEDs; Read the information provided on the VOP	Permanent Encryption Encryption Enabled Encryption Disabled	None
Power Cycle/Perform Self-Tests	Cycle the power on the module, which will invoke self-tests on power-up	Permanent Encryption Encryption Enabled Encryption Disabled	None
Reset Module IP	Reset the module's IP address to the default IP address using the recessed switch	Permanent Encryption Encryption Enabled Encryption Disabled	None
Interface Port Management	Manage the module through the Interface Port (non-security relevant)	Permanent Encryption Encryption Enabled Encryption Disabled	None
Library Management	Manage the module and retrieve status information through the TTI (non-security relevant)	Permanent Encryption Encryption Enabled Encryption Disabled	None
Operator Panel Management	Manage the module and retrieve status information through the Operator Panel port (non-security relevant)	Permanent Encryption Encryption Enabled Encryption Disabled	None

2.4.4 Non-Approved Mode Roles and Services

While operating in the non-Approved mode, operators are not required to assume an authorized role in order to access and utilize module services. Thus, all module services are available to all operators with access to the module.

When operating in the non-Approved Mode, the StorageTek T10000C Tape Drive provides a subset of the services that are available in Encryption Enabled and

Encryption Disabled Approved Modes. These services shall be considered non-compliant services. The services that are available to an operator of the ETD while it is operating in the non-Approved Mode are listed in Table 9 below.

Table 9 – non-Approved Security Services

Service	Description
Enable Encryption Disabled Mode	Turn encryption off; OKM services are enabled
Configure Module	Perform routine module configuration
Enable Encryption/Obfuscation[37]	Enable encryption/obfuscation services (without reboot)
Disable Encryption/Obfuscation	Disable encryption/obfuscation (without reboot)
Access Module via Virtual Operator's Panel (VOP)	Log into VOP and manage the module
Create Dump (Non-Encrypted)	Create non-encrypted dump file and save to EEPROM
Initial Program Load (IPL)	Reinitialize module and run self-tests
View non-Approved mode Audit Log	View, download, or delete audit log
View Drive Data	Read module configuration data
View non-Approved mode Error Log	View, download, or delete error log
Delete Dump	Delete the currently stored dump file
Delete Perms	Deletes currently stored error messages
Tape Management	Load or unload a new tape cartridge into the module
Run Diagnostics	Perform a diagnostic test on the module
Encrypt Data	Encrypt data from the module to the tape cartridge
Decrypt Data	Decrypt data read from the tape cartridge
Write Plaintext Data	Write plaintext data from the module to the tape cartridge
Read Plaintext Data	Read plaintext data from the tape cartridge
Export Keys	Export keys from the module to an external device in plaintext
Import Keys	Import keys to the module from an external device in plaintext

[37] Obfuscation of data is equivalent to plaintext output

Service	Description
Show Status	Determine the current status of the module by reading the Encryption and Drive Status LEDs; Read the information provided on the VOP
Power Cycle/Perform Self-Tests	Cycle the power on the module, which will invoke self-tests on power-up
Reset Module IP	Reset the module's IP address to the default IP address using the recessed switch
Interface Port Management	Manage the module through the Interface Port (non-security relevant)
Library Management	Manage the module and retrieve status information through the TTI (non-security relevant)
Operator Panel Management	Manage the module and retrieve status information through the Operator Panel port (non-security relevant)

2.5 Physical Security

The StorageTek T10000C Tape Drive satisfies level 1 physical security requirements by being constructed of a hard, production-grade metal exterior. The module provides an opening, which is required for the insertion of media (tape cartridges). The opening is constructed of hard, production-grade plastic. All internal hardware, firmware, and cryptographic data are protected by the enclosure of the module, which makes up its physical cryptographic boundary.

NOTE: The labels pictured in Figure 1 and Figure 2 above do not add any additional security to the module.

2.6 Operational Environment

The operational environment for the StorageTek T10000C Tape Drive consists of two ARM 926EJS processors, which are the module's only general-purpose processors. These processors execute the module's firmware (Firmware Version: 1.57.308). The module does not employ a general Operating System.

2.7 Cryptographic Key Management

The StorageTek T10000C Tape Drive was designed to operate in three FIPS-Approved modes of operation: Permanent Encryption Mode, Encryption Enabled Mode, and Encryption Disabled Mode. The following sections detail which cryptographic algorithms, keys, and CSPs are available for each FIPS-Approved mode.

2.7.1 Encryption Enabled Cryptographic Algorithm Implementations

The StorageTek T10000C Tape Drive provides access to the same cryptographic algorithms when operating in either the Permanent Encryption Approved Mode or Encryption Enabled Approved Mode. The cryptographic algorithms available in these Approved modes are listed in Table 10.

Table 10 – FIPS-Approved Algorithms in StorageTek T10000C Tape Drive (Permanent Encryption and Encryption Enabled Modes)

Algorithm	Implementation Description	Certificate Number
AES[38] 256-bit ECB[39] mode (CCM implementation)	AES in ECB mode as used in firmware AES CCM encryption with Cert # 2412	2404
AES 256-bit ECB mode (Used with OKM)	Unwrap AES Media Keys[40] being sent from the OKM	2405
AES 256-bit ECB mode (DRBG implementation)	AES in ECB mode as used with the SP[41] 800-90A CTR[42] DRBG with Cert # 322	2407
AES 256-bit CBC[43]mode (TLS[44] 1.0 implementation)	AES in CBC mode used in a TLS session between the ETD and OKM	2406
AES 256-bit ECB mode (DCCM hardware implementation)	AES in ECB mode as used in hardware AES CCM encryption with Cert # 1570	1568
AES 256-bit CCM mode (DCCM hardware implementation)	AES in CCM mode as used with AES in ECB mode with Cert # 1568	1570
AES 256-bit CCM mode (Firmware implementation)	AES in CCM mode as used with AES in ECB mode with Cert # 2404	2412
SHA[45]-1 (Firmware implementation)	Used for digital signature verification; Used with HMAC SHA-1 (Cert # 1497); User data hashing	2065
SHA-1 (TLS 1.0 implementation)	Used as part of the TLS 1.0 TLS Key Derivation Function; Used with HMAC SHA-1 (Cert # 1498)	2066
HMAC[46] SHA-1 (Used with OKM)	Create challenge responses as part of the certificate service of OKM; Used with SHA-1 (Cert #: 2065)	1497
HMAC SHA-1 (TLS 1.0 implementation)	Provides integrity during a TLS session; Used with SHA-1 (Cert # 2066)	1498

[38] AES – Advanced Encryption System
[39] ECB – Electronic Code Book
[40] Media Keys are a defined CSP. See Table 13 in VE07.03.01
[41] SP – Special Publication
[42] CTR - Counter
[43] CBC – Cipher Block Chaining
[44] TLS – Transport Layer Security
[45] SHA – Secure Hash Algorithm
[46] HMAC – (Keyed-) Message Authentication Code

Algorithm	Implementation Description	Certificate Number
RSA 2048-bit PKCS[47] #1 v1.5 Signature Verification	Verifies the signature of a new firmware image to be loaded onto the ETD; Used with SHA-1 (Cert # 2065)	1246
TLS 1.0 Key Derivation	TLS 1.0 Key Derivation (SP800-135 rev1; Section 4.2.1)	82
SP800-90A CTR DRBG	Generates random numbers for nonces and keys	322

Caveat: Additional information concerning SHA-1 and specific guidance on transitions to the use of more robust hashing algorithms is contained in NIST Special Publication 800-131A.

When operating in the Permanent Encryption and Encryption Enabled Approved Modes, the ETD wraps data it sends to an OKM cluster with AES Key Wrap. AES Key Wrap, as defined in SP 800-38F, is an approved key wrapping, key establishment methodology.

- AES (Cert #:2405, Key Wrapping provides 256 bits of encryption strength)

The following non-Approved methods are allowed for use, as described, in the Permanent Encryption and Encryption Enabled Modes:

- RSA (Key wrapping; key establishment methodology provides 112 bits of encryption strength)
- The module provides a Non-Deterministic Random Number Generator (NDRNG) as the entropy source to the FIPS-Approved SP 800-90A CTR DRBG.
- The module provides MD5 for use with TLS 1.0 protocol.

[47] PKCS – Public Key Cryptographic Standard

2.7.2 Encryption Disabled Cryptographic Algorithms

The Encryption Disabled Approved Mode utilizes a subset of the cryptographic algorithms listed in Table 10. A list of cryptographic algorithms used by the module while operating in the Encryption Disabled Mode is provided as Table 11.

Table 11 – FIPS-Approved Algorithms in StorageTek T10000C Tape Drive (Encryption Disabled Mode)

Algorithm	Implementation Description	Certificate Number
AES 256-bit ECB mode (DRBG implementation)	AES in ECB mode as used with the SP 800-90A CTR DRBG with Cert # 322	2407
SHA-1 (Firmware implementation)	Used for digital signature verification; User data hashing	2065
RSA 2048-bit PKCS #1 v1.5 Signature Verification	Verifies the signature of a new firmware image to be loaded onto the ETD; Used with SHA-1 (Cert # 2065)	1246
SP800-90A CTR DRBG	Generates random numbers for nonces and keys	322

Caveat: Additional information concerning SHA-1 and specific guidance on transitions to the use of more robust hashing algorithms is contained in NIST Special Publication 800-131A.

2.7.3 Non-Approved Mode Security Functions

The cryptographic algorithms listed in Table 12 are available to the StorageTek T10000C Tape Drive while operating in the non-Approved Mode.

Table 12 – Non-Approved Mode Security Functions

Algorithm
AES 256-bit ECB mode (Firmware; non-compliant)
AES 256-bit ECB mode (Hardware; non-compliant)
AES 256-bit CBC mode (non-compliant)
AES 256-bit CCM mode (Firmware; non-compliant)
AES 256-bit CCM mode (Hardware; non-compliant)
SHA-1 (non-compliant)
HMAC SHA-1 (non-compliant)
RSA 2048-bit PKCS #1 v1.5 Encrypt/Decrypt (non-compliant)
SP 800-90A CTR DRBG (non-compliant)

2.7.4 Encryption Enabled Cryptographic Keys and Critical Security Parameters

The cryptographic keys, key components, and other CSPs used by the module while operating in either the Permanent Encryption Approved Mode or Encryption Enabled Approved Mode are shown in Table 13.

Table 13 – List of Cryptographic Keys, Cryptographic Key Components, and CSPs (Permanent Encryption and Encryption Enabled Modes)

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
Media Key (MEKey)	AES CCM 256-bit	Generated externally; Input encrypted via AKWK	Output encrypted via DEKey	Plaintext in RAM[48] and FPGA[49]	"Reset" service; Switch Approved Mode	To encrypt and decrypt data to and from magnetic tape
AES Key Wrap Key (AKWK)	AES ECB 256-bit	Generated internally via Approved DRBG	Output encapsulated via KWKPublicKey	Plaintext in RAM	"Reset" service; Power cycle; Switch Approved Mode	Decrypt MEKey
Dump Encryption Key (DEKey)	AES CCM 256-bit	Generated internally via Approved DRBG	Output encrypted via DEPubKey	Plaintext in RAM	"Reset" service; Power cycle; Switch Approved Mode	Encrypt dump files
Dump Encryption Public Key (DEPubKey)	RSA 2048-bit public key	Generated externally; Hardcoded into module	Does not exit the module	Plaintext in EEPROM	Not Applicable	Encapsulate DEKey
Tape Drive Private Key (TDPrivKey)	RSA 2048-bit private key	Generated externally; Input via TLS_ECK	Output encrypted via DEKey	Plaintext in RAM and EEPROM	"Reset" service; Switch Approved Mode	Authenticate the module to OKM cluster appliance during TLS session
Tape Drive Public Key (TDPubKey)	RSA 2048-bit public key	Generated externally; Input via TLS_ECK	Output encrypted via DEKey; Output in plaintext	Plaintext in EEPROM	"Reset" service; Switch Approved Mode	Authenticate the module to OKM cluster appliance during TLS session

[48] RAM – Random Access Memory
[49] FPGA – Field Programmable Gate Array

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
TLS_PM	48 bytes random data	Generated internally via Approved DRBG	Output encapsulated via CA_Cert	Plaintext in RAM	"Reset" service; Power cycle; Switch Approved Mode	Premaster secret for TLS 1.0 session
TLS_MS	48 bytes pseudo-random data	Generated internally via TLS 1.0 PRF[50]	Does not exit the module	Plaintext in RAM	"Reset" service; Power cycle; Switch Approved Mode	Master secret for TLS 1.0 session
TLS_EMK	HMAC SHA-1	Generated internally via TLS 1.0 PRF	Does not exit the module	Plaintext in RAM	"Reset" service; Power cycle; Switch Approved Mode	Authentication key for data leaving the module (per TLS 1.0)
TLS_DMK	HMAC SHA-1	Generated internally via TLS 1.0 PRF	Does not exit the module	Plaintext in RAM	"Reset" service; Power cycle; Switch Approved Mode	Authentication key for data entering the module (per TLS 1.0)
TLS_ECK	AES CBC 256-bit	Generated internally via TLS 1.0 PRF	Does not exit the module	Plaintext in RAM	"Reset" service; Power cycle; Switch Approved Mode	Encryption key for data leaving the module (per TLS 1.0)
TLS_DCK	AES CBC 256-bit	Generated internally via TLS 1.0 PRF	Does not exit the module	Plaintext in RAM	"Reset" service; Power cycle; Switch Approved Mode	Decryption key for data entering the module (per TLS 1.0)
CA_Cert	RSA 2048-bit public Key	Generated externally. Input in plaintext via CA[51]	Output encrypted via DEKey	Plaintext in EEPROM	"Reset" service; Switch Approved Mode	Authenticate the OKM cluster appliance to the module during TLS session
Key Wrap Key Public Key (KWKPublicKey)	RSA 2048-bit public key	Generated externally; Input encrypted via TLS_ECK	Output encrypted via DEKey	Plaintext in EEPROM	"Reset" service; Switch Approved Mode	Wrap AKWK to be sent to OKM cluster

[50] PRF (Pseudo Random Function) is based on a hash on the TLS_PM and nonces; Utilizes SHA-1 and MD5 (Message Digest 5)

[51] CA – Certificate Authority

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
Firmware Signature Public Key (FSPubKey)	RSA 2048-bit public key	Generated externally; Hardcoded into module	Does not exit the module	Plaintext in EEPROM	Not Applicable	Validate a new firmware image loaded onto module
Firmware Signature Root Certificate Key (FSRootCert)	RSA 2048-bit public key	Generated externally; Hardcoded into module	Does not exit the module	Plaintext in EEPROM	Not Applicable	Verify the chain of certificates provided by the new firmware image

DRBG Seed	Random bit value	Generated internally	Does not exit the module	Plaintext in RAM	"Reset" service;
					Power cycle;
					Switch Approved Mode
						Generate random values for the CTR_DRBG

DRBG 'V' Value	Internal DRBG state value (integer)	Generated internally	Does not exit the module	Plaintext in RAM	"Reset" service;
					Power cycle;
					Switch Approved Mode
						Internal state value for the CTR_DRBG

DRBG 'Key' Value	Internal DRBG state value (integer)	Generated internally	Does not exit the module	Plaintext in RAM	"Reset" service;
					Power cycle;
					Switch Approved Mode
						Internal state value for the CTR_DRBG

*The vendor makes no conformance claims to any key derivation function specified in SP 800-135rev1. References to the TLS key derivation function addressed in SP 800-135rev1 is only listed to clarify the key types supported by ETD.

2.7.5 Encryption Disabled Cryptographic Keys and Critical Security Parameters

The cryptographic keys, key components, and other CSPs used by the module while operating in the Encryption Disabled Approved Mode are shown in Table 14.

Table 14 – List of Cryptographic Keys, Cryptographic Key Components, and CSPs (Encryption Disabled Mode)

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
Dump Encryption Public Key (DEPubKey)	RSA 2048-bit public key	Generated externally; Hardcoded into module	Does not exit the module	Plaintext in EEPROM	Not Applicable	Not used in the Encryption Disabled Mode

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
Firmware Signature Public Key (FSPubKey)	RSA 2048-bit public key	Generated externally; Hardcoded into module	Does not exit the module	Plaintext in EEPROM	Not Applicable	Validate a new firmware image loaded onto module
Firmware Signature Root Certificate Key (FSRootCert)	RSA 2048-bit public key	Generated externally; Hardcoded into module	Does not exit the module	Plaintext in EEPROM	Not Applicable	Verify the chain of certificates provided by the new firmware image

2.8 EMI/EMC

The StorageTek T10000C Tape Drive conforms to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (business use).

2.9 Self-Tests

The StorageTek T10000C Tape Drive performs the required Integrity Test and Power-On Self-Tests (POSTs) during initial power-up. On-demand self-tests can be performed by the "IPL" service available to the CO or by cycling the power of the module. The module executes conditional self-tests during normal operation whenever a new random number is generated or whenever new firmware is loaded. The following sections describe the power-up and conditional self-tests that are run by the module in each Approved mode.

2.9.1 Integrity Tests

An integrity test is the first operation performed by the StorageTek T10000C Tape Drive after power has been supplied. The module performs a 32-bit CRC[52] on the firmware as its approved integrity technique. Data output is not available while the integrity test is being performed. If the test passes, the module will continue on to perform the required Known Answer Tests (KATs) on its cryptographic algorithms. If the firmware integrity test fails, the module will remain in its initial boot state and create an unencrypted dump file[53]. The CO will be required to reboot the module in order to resolve the error.

2.9.2 Power-On Self-Tests

POSTs are performed by the ETD when power is applied to the module and after the integrity test has passed. Data output is not available while the POSTs are being performed. After the POSTs successfully complete, the module will begin normal operation. Normal operation may be in one of the three Approve modes or in the non-Approved mode. The operational status of the module is determined when the module first boots. If any of the POSTs fail, then the ETD will create an unencrypted dump file and then continue to reboot.

The following POSTs are performed by the module during every boot-up, regardless of current operational mode:

- AES ECB KAT
- AES CBC KAT

[52] CRC – Cyclic Redundancy Check

[53] When operating in the Permanent Encryption or Encryption Enabled Modes, unencrypted data dumps shall be deleted by the CO after their creation

- AES CCM KAT (Firmware)
- AES CCM KAT (Hardware)
- AES Key Wrap KAT
- RSA Signature Verification KAT with a 2048-bit precomputed signature
- RSA Encrypt/Decrypt KAT
- SHA-1 KAT
- SHA-1 KAT (TLS)
- HMAC SHA-1 KAT
- HMAC SHA-1 KAT (TLS)
- SP 800-90A CTR DRBG KAT

2.9.3 Conditional Self-Tests

When operating in the Permanent Encryption and Encryption Enabled Approved Modes, the StorageTek T10000C Tape Drive performs a Continuous Random Number Generator Test (CRNGT) on the output from the DRBG each time a new random number is generated. In addition, a CRNGT is performed on the output from the NDRNG prior to being used as entropy input for the DRBG. If any of the CRNGTs fail, the module will generate a dump file and attempt to perform the CRNGT a second time. If the CRNGT passes on the second attempt, the ETD will encrypt the dump file and then reboot. If the CRNGT fails on the second attempt, the dump file is discarded and the module will then reboot.

In each of the Approved Modes, a firmware load test is performed on new firmware being loaded onto the module. Firmware can be loaded onto the module via the Host Interface or via the Tape Head interface. The ETD uses a 2048-bit RSA digital signature verification to confirm the integrity of the firmware prior to being loaded onto the module. If the test passes, the module will reboot and the new firmware will be used. If the test fails, the new firmware image will be discarded and the module will resume normal operation. Firmware is unable to be loaded into the module while operating in the non-Approved Mode.

2.9.4 Critical Functions Tests

When operating in the Permanent Encryption and Encryption Enabled Approved Modes, critical function self-tests are required by the module when operating the SP 800-90A CTR DRBG. Critical functions tests are crucial for the proper and secure operation of the DRBG. These tests will ensure the DRBG always produces random information.

The StorageTek T10000C Tape Drive performs the following critical function self-tests:

- SP 800-90A DRBG Instantiate Test

- SP 800-90A DRBG Reseed Test
- SP 800-90A DRBG Uninstantiate Test

2.10 Mitigation of Other Attacks

This section is not applicable. The module does not claim to mitigate any attacks beyond the FIPS 140-2 Level 1 requirements for this validation.

3 SECURE OPERATION

The Oracle StorageTek T10000C Tape Drive meets Level 1 requirements for FIPS 140-2. This section provides Cryptographic Officer guidance for the proper use and maintenance of the module. Instructions for placing the module into one of the three Approved modes are also provided. Operators of the ETD should read and be familiar with the following Oracle documents prior to configuring and operating the module.

- *StorageTek T10000 Tape Drive Operator's Guide* (Part#: E20714-04; April 2013)
- *StorageTek Virtual Operator Panel: User's Guide (Customer Version)* (Part #: E37053-01; September 2012)
- *Oracle Key Manager: Administration Guide* (Part #: E26025-03; January 2011)

Prior to setting up the StorageTek T10000C Tape Drive for first use, the CO shall use the instructions provided in these guides to install the latest versions of Oracle Key Manager and the Virtual Operator Panel onto a trusted system. These external software components are required for setting up the ETD for normal operation.

3.1 Cryptographic Officer Guidance (First Use)

This section provides instructions on how to place the StorageTek T10000C Tape Drive into each of the three FIPS-Approved modes after first receiving the drive from Oracle Corporation. For first-time use, these operations shall be performed with an Oracle Service Representative present.

3.1.1 Initial Set-Up

Prior to placing the module into one of the three Approved modes, the CO shall perform the following steps:

1. Install the StorageTek T10000C Tape Drive following the instruction provided in *StorageTek T10000 Tape Drive Installation Guide*
2. Examine the hardware part number on the rear label. Confirm it matches the hardware version number on this Security Policy (Hardware Part #: 7054185)
3. Using VOP, the CO shall check the Version Tab (Retrieve →View Drive Data) to confirm the current firmware version number matches the firmware version number listed on this Security Policy (Firmware Version: 1.57.308)
4. The CO shall set the drive to an "offline" state (Drive Operations → Set Offline)

3.1.2 Encryption Disabled Approved Mode Set-Up

The StorageTek T10000C Tape Drive is initially delivered to an Oracle customer with the Encryption Disabled Mode configured. Upon first receiving the ETD, the CO shall perform the following steps to ensure the module is operating in the Encryption Disabled Mode:

1. Follow the steps outlined in Section 3.1.1 (*Initial Set-Up*)
2. Using VOP, navigate to the “Encrypt” tab in the “Drive Data” window (Configure → Drive Data)
3. Verify that the “Use KMS or DPKM” Field is set to “UNKN”
    a. Set the “Use KMS or DPKM” Field to “UNKN” if not previously set
4. Press the “Commit” button

After pressing the “Commit” button, the ETD will reboot to normal operation. From this point forward, the module will be operating in the Encryption Disabled Approved Mode.

3.1.3 Encryption Enabled Approved Mode Set-Up

To place the StorageTek T10000C Tape Drive into the Encryption Enabled Mode, the CO shall perform the following steps:

1. Follow the steps outlined in Section 3.1.1 (*Initial Set-Up*)
2. Using OKM, the CO shall add the ETD to the OKM cluster
3. Using VOP, navigate to the “Encrypt” tab in the “Drive Data” window (Configure → Drive Data)
4. Set the “Use KMS or DPKM” Field to “KMS”
5. Set the “Permanently encrypting” field to “No”
6. Enter a valid Agent ID, Pass Phrase, and OKM IP Address
7. Press the “Commit” button

After pressing the “Commit” button, the ETD will reboot to normal operation. From this point forward, the module will be operating in the Encryption Enabled Approved Mode.

3.1.4 Permanent Encryption Approved Mode Set-Up

To place the StorageTek T10000C Tape Drive into the Permanent Encryption Mode, the CO shall perform the following steps:

1. Follow the steps outlined in Section 3.1.1 (*Initial Set-Up*)
2. Using OKM, the CO shall add the ETD to the OKM cluster
8. Using VOP, navigate to the “Encrypt” tab in the “Drive Data” window (Configure → Drive Data)
3. Set the “Use KMS or DPKM” Field to “KMS”
4. Set the “Permanently encrypting” field to “Yes”
5. Enter a valid Agent ID, Pass Phrase, and OKM IP Address
6. Press the “Commit” button

After pressing the “Commit” button, the ETD will reboot to normal operation. From this point forward, the module will be operating in the Permanent Encryption Approved Mode. Once operating in this mode, the module will be unable to operate in any other Approved or non-Approved modes.

3.2 Cryptographic Officer Guidance (Normal Operation)

This section assumes the StorageTek T10000C Tape Drive has been placed into one of the three FIPS-Approved modes or the non-Approved Mode. Instructions on how to place the drive into another mode are provided in this section. The CO is responsible for placing the ETD into one of the three Approved modes of operation. An Oracle Service Representative is not required to be present when switching Approved modes. Switching to one of the defined Approved modes from the non-FIPS-Approved mode will cause keys generated in the non-Approved mode to be zeroized.

3.2.1 Switching To Encryption Disabled Approved Mode

The CO can place the module into the Encryption Disabled Mode from the Encryption Enabled Mode or the non-Approved Mode. The CO shall perform the following steps to place the module into the Encryption Disabled Mode:

1. Using the “Drive Operations” menu on VOP, reset the ETD[54]
2. After reboot, use the “Drive Operations” menu to place the drive offline
3. Navigate to the “Encrypt” tab in the “Drive Data” window (Configure → Drive Data)
4. Set the “Turn encryption off” field to “Yes”
5. Press the “Commit” button

After pressing the “Commit” button, the ETD will reboot to normal operation. From this point forward, the module will be operating in the Encryption Disabled Approved Mode.

3.2.2 Switching To Encryption Enabled Approved Mode

The CO can place the module into the Encryption Enabled Mode from the Encryption Disabled Mode. The CO shall perform the following steps to place the module into the Encryption Enabled Mode:

1. Using the “Drive Operations” menu on VOP, place the drive offline
2. Navigate to the “Encrypt” tab in the “Drive Data” window (Configure → Drive Data)
3. Set the “Use KMS or DPKM” field to “KMS”
4. Set the “Permanently encrypting” field to “No”
5. Enter a valid Agent ID, Pass Phrase, and OKM IP Address
6. Press the “Commit” button

[54] Step 1 is not required if the drive is currently operating in the Non-Approved Mode

After pressing the “Commit” button, the ETD will reboot to normal operation. From this point forward, the module will be operating in the Encryption Enabled Approved Mode.

3.2.3 Switching To Permanent Encryption Approved Mode

The CO can place the module into the Permanent Encryption Mode from the Encryption Disabled Mode or the Encryption Enabled Mode. The CO shall perform the following steps to place the module into the Permanent Encryption Mode:

1. Using the “Drive Operations” menu on VOP, reset the ETD[55]
2. Using “Drive Operations” menu on VOP, place the drive offline
3. Navigate to the “Encrypt” tab in the “Drive Data” window (Configure → Drive Data)
4. Set the “Use KMS or DPKM” field to “KMS”
5. Set the “Permanently encrypting” field to “Yes”
6. Enter a valid Agent ID, Pass Phrase, and OKM IP Address
7. Press the “Commit” button

After pressing the “Commit” button, the ETD will reboot to normal operation. From this point forward, the module will be operating in the Permanent Encryption Approved Mode. Once operating in this mode, the module will be unable to operate in any of the other two Approved modes or the non-Approved Mode.

3.3 Cryptographic Officer Guidance (Non-Approved Mode)

The StorageTek T10000C Tape Drive is capable of operating in a non-FIPS-Approved mode of operation. This section provides instructions on how to enable the non-Approved Mode on first use of the ETD as well as from the Encryption Enabled and Encryption Disabled Modes. Switching to the non-FIPS-Approved mode will cause the module to zeroize all CSPs.

3.3.1 Enable non-Approved Mode (First Use)

The CO can place the StorageTek T10000C Tape Drive into the non-Approved Mode after initially receiving the ETD. The CO shall perform the following steps:

1. Follow the steps outlined in Section 3.1.1 (*Initial Set-Up*)
2. Using VOP, navigate to the “Encrypt” tab in the “Drive Data” window (Configure → Drive Data)
3. Set the “Use KMS or DPKM” field to “DPKM”

[55] This step is not needed if the drive is currently operating in the Encryption Disabled Mode

4. Press the “Commit” button

After pressing the “Commit” button, the ETD will reboot to normal operation. From this point forward, the module will be operating in the non-Approved Mode.

3.3.2 Switching To non-Approved Mode

The CO can place the module into the non-Approved Mode from the Encryption Disabled Mode. The CO shall perform the following steps to place the module into the non-Approved Mode:

1. Using “Drive Operations” menu on VOP, reset the ETD
2. After reboot, use the “Drive Operations” menu to place the drive offline
3. Navigate to the “Encrypt” tab in the “Drive Data” window (Configure → Drive Data)
4. Set the “Use KMS or DPKM” field to “DPKM”
5. Set the “Permanently encrypting” field to “UNKN”
6. Press the “Commit” button

After pressing the “Commit” button, the ETD will reboot to normal operation. From this point forward, the module will be operating in the non-Approved Mode.

3.4 Zeroization

Zeroization of the module’s Critical Security Parameters shall be done under direct control of the Cryptographic Officer. Zeroization can be accomplished by the CO performing the Reset service. The module will also perform zeroization automatically when switching between the Approved modes and to and from the non-Approved mode.

4 ACRONYMS

Acronyms used within this document are listed below.

AES	Advanced Encryption Standard
AKWK	AES Key Wrap Key
CA	Certificate Authority
CBC	Cipher-Block Chaining
CCM	Counter with CBC-MAC
CMVP	Cryptographic Module Validation Program
CO	Cryptographic Officer
CRC	Cyclic Redundancy Check
CRNGT	Continuous Random Number Generator Test
CSEC	Communications Security Establishment Canada
CSP	Critical Security Parameter
CTR	Counter
DPKM	Data Path Key Management
DRBG	Deterministic Random Bit Generator
ECB	Electronic Codebook
EEPROM	Electronically Erasable Programmable Read-Only Memory
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ETD	Encrypting Tape Drive
FC-SB-3	Fibre Channel Single-Byte-3
FCP-3	Fibre Channel Protocol-3
FICON	Fibre Connection
FIPS	Federal Information Processing Standard
FPGA	Field Programmable Gate Array
GUI	Graphical User Interface
HMAC	(Keyed-) Hash-based Message Authentication Code
Hz	Hertz
IP	Internet Protocol
IPL	Initial Program Load
KAT	Known Answer Test
KMA	Key Management Appliance
KMS	Key Management System
LCD	Liquid Crystal Display
LED	Light Emitting Diode
MB	Megabytes
MD5	Message Digest Algorithm 5
NDRNG	Non-Deterministic Random Number Generator
NIST	National Institute of Standards and Technology
OKM	Oracle Key Manager
PKCS	Public Key Cryptography Standards
POST	Power-On Self-Test
PRF	Pseudo-Random Function
RAM	Random Access Memory
RFID	Radio Frequency Identification
RJ	Registered Jack
RS	Recommended Standard

RSA	Rivest, Shamir, Adleman
SCSI	Small Computer System Interface
sec	Second
SNMP	Simple Network Management Protocol
SP	Special Publication
SSC-3	SCSI Stream Commands-3
SHA	Secure Hash Algorithm
TLS	Transport Layer Security
TTI	Tape Transport Interface
UNKN	Unknown
VAC	Volts Alternating Current
VOP	Virtual Operator Panel