



StorageTek™ T10000C

Tape Drive

Security Policy

Part Number 316052503

Revision: 1.5

June 2011

Copyright © 2011, Oracle and/or its affiliates. All rights reserved. Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners. This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

1 MODULE OVERVIEW 4

2 SECURITY LEVEL 7

3 MODES OF OPERATION (AREA 1) 8

 3.1 APPROVED ALGORITHMS 8

 3.2 NON-APPROVED ALGORITHMS 9

 3.3 DETERMINING FIPS MODE 9

 3.4 CONFIGURING THE DRIVE IN FIPS MODE 10

4 PORTS AND INTERFACES 10

5 IDENTIFICATION AND AUTHENTICATION POLICY 13

 5.1 ASSUMPTION OF ROLES 13

6 DEFINITION OF CRITICAL SECURITY PARAMETERS (CSPS) 13

 6.1 DEFINITION OF PUBLIC KEYS 14

7 ACCESS CONTROL POLICY 15

 7.1 ROLES AND SERVICES 15

8 OPERATIONAL ENVIRONMENT (AREA 6) 20

9 SECURITY RULES 20

 9.1 FIPS 140-2 SECURITY REQUIREMENTS 20

10 PHYSICAL SECURITY 21

 10.1 PHYSICAL SECURITY MECHANISMS 21

11 MITIGATION OF OTHER ATTACKS POLICY 22

12 REFERENCES 22

13 DEFINITIONS AND ACRONYMS 23

TABLE OF TABLES

TABLE 1: MODULE SECURITY LEVEL SPECIFICATION 7

TABLE 2: PORTS AND INTERFACES DESCRIPTION 10

TABLE 3: ROLES 13

TABLE 4: DESCRIPTION OF CRITICAL SECURITY PARAMETERS (CSPS) 13

TABLE 5: DESCRIPTION OF PUBLIC KEYS WITHIN THE ETD 14

TABLE 6: SERVICES AUTHORIZED FOR ROLES 15

TABLE 7: NO ROLE SERVICES 19

Release History

Date	Rev	Description	Name
02/05/10	AA	Initial version of Security Policy. Engineering Change: EC001056	Matt Ball
02/16/10	1.0	Changed policy per Infogard comments for T10000C	Ben Baron
02/25/10	1.1	Changed policy per Infogard comments for T10000C	Ben Baron
03/29/11	1.2	Oracle updates and document corrections	Linda Gallops
03/30/11	1.3	Added photos per InfoGard request	Ben Baron
04/05/11	1.4	Fixed fonts and referencing as requested by InfoGard and corrected formatting	Linda Gallops
06/01/11	1.5	Minor changes and photos added as requested by InfoGard	Linda Gallops

1 Module Overview

The StorageTek™ T10000C Tape Drive by Oracle Corporation (“Encrypting Tape Drive”, or ETD) (HW P/N: 316052503; Firmware Version: 1.51.318) 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 on magnetic tape.

The ETD is intended to be used in conjunction with the Oracle Key Manager, which provides centralized key management. The Oracle Key Manager (formerly called the Key Management System 2, or KMS 2) consists of two or more Key Management Appliances (KMAs). Key Management Appliances are the individual components within the system and in the context of this FIPS 140-2 Security Policy, can be viewed as Key Loaders. For more information on these system components please see the website <http://www.oracle.com/technetwork/indexes/documentation/index.html>. From the main Website the user selects Storage -> Tape Storage and under Tape Drives selects StorageTek T9x40 and T10000.

The cryptographic boundary of the ETD is the external surface of the tape drive’s commercial-grade metallic enclosure. Figures 1.1 – 1.6 illustrate the cryptographic boundary as defined. Note: Figure 1.2 appears to be upside-down to show bottom plate.

Figure 1.1: Front of T10000C



Figure 1.2: Bottom of T10000C



Figure 1.3: Top of T10000C



Figure 1.4: Rear of T10000C



Figure 1.5: Right side of T10000C



Figure 1.6: Left side of T10000C



2 Security Level

The ETD meets the overall requirements applicable to Level 1 security of FIPS 140-2, as is detailed in Table 1.

Table 1: Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	1
Module Ports and Interfaces	1
Roles, Services and Authentication	1
Finite State Model	1
Physical Security	1
Operational Environment	N/A

Security Requirements Section	Level
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A

3 Modes of Operation (Area 1)

3.1 Approved Algorithms

Once configured per the procedures as defined in Section 3.4 the module is only able to operate in a FIPS 140-2 Approved Mode of operation. Within the FIPS 140-2 Approved Mode of operation the following Approved algorithms are available:

1. AES #1564: T10000C AES used in CCM
 2. AES #1565: T10000C KMS Agent AES
 3. AES #1566: T10000C AES used in CTR DRBG
 4. AES #1567: T10000C AES used in TLS1.0
 5. CCM #1569: T10000C CCM Firmware Implementation
 6. DRBG #71: T10000C CTR DRBG
 7. HMAC #916: T10000C HMAC KMS Agent
 8. HMAC #917: T10000C HMAC used in TLS1.0
 9. RSA #763: T10000C RSA SigVerPKCS1.5
 10. SHA #1389: T10000C SHA-1
 11. SHA #1390: T10000C SHA-1 used in TLS1.0
 12. AES #1568: T10000C AES Hardware Implementation
 13. CCM #1570: T10000C CCM Hardware Implementation
- AES CCM supporting 256-bit keys in both hardware (AES Certificate # 1568) (CCM Certificate #1570) and firmware (AES Certificate # 1564) (CCM Certificate #1569).
 - AES ECB encryption (AES Certificate # 1565) as used in CCM encryption in firmware (AES Certificate # 1564, as above).
 - RSASSA-PKCS1-v1_5 supporting 2048-bit keys (RSA Certificate # 763) for digital signature verification (firmware load test).
 - HMAC SHA-1 (HMAC Certificate # 916) to create the challenge response as part of the certificate service of the KMS 2.x Agent Toolkit.

- SHA-1 (SHS Certificate # 1389) for the following:
 - as part of digital signature verification for the firmware
 - as part of HMAC-SHA-1 (HMAC certificate # 916, as above)
 - for hashing passwords used for authentication
- AES ECB (AES Certificate # 1567) supporting 256-bit keys. Used as part of the AES Key Wrap algorithm to securely establish keying material.
- SP 800-90 CTR DRBG (DRBG Certificate # 71) for generating random numbers used for nonce values and cryptographic keys.
- AES CTR (AES Certificate # 1566) as part of the SP 800-90 CTR DRBG.
- AES CBC mode with 256-bit key (AES Certificate # 1567), used within TLS session between ETD and KMS 2.x.
- HMAC-SHA-1 (HMAC Certificate # 917) with 160-bit key used to protect the integrity of TLS communications between the ETD and KMS 2.x.
- SHA-1 (SHS Certificate #1390)
 - as part of the TLS Key Derivation Functionality.
 - as part of HMAC SHA-1 (HMAC Certificate # 917, as above).

3.2 Non-Approved Algorithms

The cryptographic module supports the following Non-Approved algorithms that are allowed for use within FIPS Approved mode: AES Key Wrap (AES Certificate #1567) used to securely establish media keys (Vendor Affirmed, key establishment methodology provides 256 bits of strength).

- RSAES-PKCS1-V1_5 supporting 2048-bit keys, for RSA public key encryption used to provide FIPS 140-2 allowed key transport within the TLS protocol. Key establishment methodology provides 112 bits of security.
- Non-Deterministic Random Number Generator (NDRNG) (provides entropy input to the SP800-90 DRBG, and random values for use within the TLS protocol).
- MD5, as used in the TLS protocol.

3.3 Determining FIPS Mode

The user can determine whether the ETD is operating in FIPS mode by examining the VOP (Virtual Operator Panel). VOP is an external software application and the primary ETD remote management tool. VOP utilizes ETD services remotely. VOP is described in more detail in the document "Virtual Operator Panel User's Guide" (see [VOPUG]).

The user can tell if the ETD is configured for an Approved mode of operation by verifying that the labels

"Encryption active" and "Running in FIPS mode" are both set to "Yes". If either of these labels is set to "No" then the ETD is not in a FIPS Approved mode.

3.4 Configuring the Drive in FIPS mode

An ETD can only be configured for FIPS mode as a one-time decision taken during the encryption enrollment process. Once an ETD is licensed for encryption, it will remain in either FIPS mode or non FIPS compliant mode.

FIPS 140-2 configuration of ETD with VOP requires the presence of both an Oracle service representative and the customer. In addition they will need to follow the licensing process as outlined in [KMS2IM] the *Oracle Key Manager Administration Guide*.

Both the Oracle service representative and the customer (in the role of the Crypto-Officer) shall perform the following actions to enable FIPS mode through VOP:

1. The service representative shall examine the hardware part number on the rear label of the Tape Drive to ensure that it matches the part number as listed in Section 1 of this document.
2. The service representative shall, using VOP, click on the menu item Drive Operations → View Drive Data.
3. The service representative shall select the Version Tab and verify that the firmware version listed is that listed in Section 1 of this document.
4. The service representative shall license the tape drive for encryption using the process from [KMS2IM].
5. The service representative shall set the drive offline by selecting Drive Operations → Set Offline.
6. The service representative shall add the ETD to the KMS 2.x cluster (see [KMS2IM]).
7. The service representative shall bring up the "Configure Drive Parameters" Window by selecting "Drive Data" from the Configure menu of the main VOP window, and in this window the customer (in the role of the Crypto-Officer) shall perform the following:
 - a) Set the "Encryption Mode" field to "Yes".
 - b) Set the "Permanently encrypting" field to "Yes".
 - c) Set the "Set FIPS mode (permanent)" field to "On".
 - d) Enter a valid Agent ID, Pass Phrase, and KMS 2.x IP address (see [KMS2IM]).
8. Click on the "Commit" button. The ETD will then reboot and come up in permanent FIPS mode.
9. Verify that FIPS mode was correctly set by examining the FIPS status (see Section 3.3).
10. The end user must not use SSL 2.0 or SSL 3.0 for secure communications.

4 Ports and Interfaces

This section describes all ports and interfaces supported by the Encrypting Tape Drive. Table 2 below provides a listing of the module's physical ports and logical interfaces (see [ETDOG] for details).

Table 2: Ports and Interfaces Description

Physical Port	Qty	Logical interface definition	Technical Specification
DB15(RS232)	1	data output, status output, control input	<p>Primarily used for tape library communications.</p> <p>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 status messages indicating failure and success.</p>
Host Interface	2	data input, data output, status output, control input	<p>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. For details, see [ETDIM].</p> <p>The interface can be configured to support one of two protocols:</p> <ol style="list-style-type: none"> 1) Fibre Channel, in accordance with the Fibre Channel Protocol-3 (FCP-3), SCSI Primary Commands-3 (see [SPC-3]), and SCSI Stream Commands (SSC-3) specifications (see [SSC-3]) 2) FICON, in accordance with the Fibre Channel Single-Byte Command Code Sets-3 Mapping Protocol (FC-SB-3), Revision 1.6 specification (see [FC-SB-3])
Tape head	1	data input, data output	<p>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.</p> <p>Tape media resides in six possible cartridge types:</p> <ol style="list-style-type: none"> 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).

Physical Port	Qty	Logical interface definition	Technical Specification
Operator Panel Port	1	status output, control input	<p>The Bottom cover of the ETD has an Operator Panel connector carrying the following signals:</p> <p>A. Four signals to provide status output:</p> <ol style="list-style-type: none"> 1. Power Indicator output signal 2. Activity Indicator output signal 3. Clean Indicator output signal 4. Service Indicator output signal <p>B. An LCD display output interface. The LCD is used to display ETD status and configuration menu text.</p> <p>C. Four switch signals (input).</p> <ol style="list-style-type: none"> 1. IPL Switch 2. Unload Switch 3. Menu Switch 4. Select Switch
Power Interface	1	power input	100-240 VAC @ 50-60 Hz
Drive Status LED	1	status output	<p>Provides status on the overall state of the ETD</p> <p>The Tape Drive's user manual includes information regarding the different status that is provided by the drive through the LEDs.</p>
Encryption Status LED	1	status output	Provides status on the encryption configuration of the ETD.
RJ45(Ethernet)	1	data input, data output, status output, control input	<p>This primary uses of this interface are to:</p> <ol style="list-style-type: none"> 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 server.

5 Identification and Authentication Policy

5.1 Assumption of roles

The ETD cryptographic module supports two distinct operator roles, User and Crypto-Officer (C.O.). Table 3 shows these roles. The module only supports six operator sessions at one time.

Table 3: Roles

Role	Type of Authentication	Authentication Data
User	None	None
Crypto-Officer	None	None

6 Definition of Critical Security Parameters (CSPs)

Table 4 describes the CSPs that are contained within the ETD.

Table 4: Description of Critical Security Parameters (CSPs)

CSP	Description/Usage
Media Key (MEKey)	Media Keys are 256-bit AES CCM keys which are generated outside the Tape Drive by the KMS 2.x. An ETD uses an MEKey to encrypt and decrypt the customer bulk data it processes.
CTR_DRBG	AES-256 key used by SP 800-90 CTR DRBG, along with the 128-bit value V , and reseed counter. Used to generate random numbers used for nonce values and cryptographic keys.
AES Key Wrap Key (AKWK)	An AES Key Wrap Key is a 256-bit AES ECB key used to protect the MEKeys with AES Key Wrap as they enter the ETD. Transported wrapped with the KWKPublicKey, which provides 112 bits of encryption strength.

CSP	Description/Usage
Dump Encryption Key (DEKey)	A Dump file encryption key is a 256-bit AES CCM key used for encrypting the dump files during generation and storage. Transported wrapped with the KWKPublicKey, which provides 112 bits of encryption strength.
Tape Drive Private Key (TDPrivKey)	The Tape Drive Private Key is a 2048-bit RSA private key used during the TLS handshake to authenticate the Tape Drive to an appliance within a KMS 2.x cluster.
TLS_PM	Premaster Secret for the TLS session. It consists of 2 bytes of version number concatenated with 46 bytes of random data.
TLS_MS	Master Secret for the TLS session; 48 bytes of pseudo-random data generated according to TLS, based on a hash of the premaster secret and nonces.
TLS_EMK	Encrypt MAC Key for TLS, used with HMAC-SHA-1 (160 bits).
TLS_DMK	Decrypt MAC Key for TLS, used with HMAC-SHA-1 (160 bits).
TLS_ECK	Encrypt Crypto Key for TLS. 256-bit key used in AES-CBC mode to encrypt TLS data.
TLS_DCK	Decrypt Crypto Key for TLS. 256-bit key used in AES-CBC mode to decrypt TLS data.

6.1 Definition of Public Keys

Table 5 describes the public keys stored with the ETD.

Table 5: Description of Public Keys within the ETD

Public Key Name	Description
CA_Cert	CA Certificate public key self-signed by a KMS 2.x cluster. Contains a 2048-bit RSA Public Key for each appliance in a KMS 2.x cluster. Used by the ETD to authenticate the appliance during the TLS handshake.
Tape Drive Public Key (TDPubKey)	The Tape Drive Public Key is a 2048-bit RSA key used by TLS. The ETD sends this key to the KMS 2.x cluster to authenticate the Tape Drive during the TLS handshake. It is stored within an X.509 certificate within the ETD.
Key Wrap Key Public Key	The Key Wrap Key Public Key is a 2048-bit RSA public key used to wrap the

Public Key Name	Description
(KWKPublicKey)	AES Key Wrap Key.
Dump Encryption Public Key (DEPubKey)	The Dump Encryption Public Key is a 2048-bit RSA public key used to wrap the DEKey. It is stored in an X.509 certificate.
Firmware Signature Public Key (FSPubKey)	The Firmware Signature Public Key is a 2048-bit RSA key used to validate any uploaded firmware.
Firmware Signature Root Certificate Key (FSRootCert)	The Firmware Signature Root Certificate Key is a 2048-bit RSA key within a PEM encoded certificate used to validate the certificate chain within the candidate firmware image.

7 Access Control Policy

7.1 Roles and Services

Table 6 shows the services available to each authorized role and CSP access (Crypto-Officer (C.O.), or User). See Section 6 for a description of the keys and CSPs.

Table 6: Services Authorized for Roles

Name of Service	Service Description	Available on:	Available in FIPS mode	Available in non-FIPS mode	Role	Access to Keys/CSPs
Enroll ETD	Authenticates an external management system acting on behalf of the Crypto-Officer (KMS 2.x cluster) to the ETD using the Passphrase.	RJ45 (Ethernet)	Yes	Yes	C.O.	Uses Passphrase; Writes and uses CA_Cert; Writes TDPPrivKey; Writes TDPubKey

Name of Service	Service Description	Available on:	Available in FIPS mode	Available in non-FIPS mode	Role	Access to Keys/CSPs
License ETD	This service is used in the VOP to enable the ETD encryption feature.	RJ45 (Ethernet)	Yes	Yes	C.O.	Uses PCKey; Uses VOP Login/password;
Load Firmware	Updates the ETD firmware.	RJ45 (Ethernet), Tape Head, Host Interface	Yes	Yes	C.O.	Writes and Uses FSPubKey; Uses FSRootCert; Writes public keys stored in firmware
Reset	This service erases all keys from ETD memory (volatile and non-volatile).	RJ45 (Ethernet)	Yes	Yes	C.O.	Zeroizes all CSPs
VOP Login	Log in to the Virtual Operator's Panel (VOP) and authorizes the operator to the Crypto-Officer Role, providing access to all VOP commands.	RJ45 (Ethernet)	Yes	Yes	C.O.	Accesses VOP Password
Encrypt Data to Tape	Encrypts data from the Host Interface on to the tape cartridge.	Tape Head, Host Interface	Yes	Yes	User	Uses MEKey
Decrypt Data from Tape	Decrypts data from the tape cartridge.	Tape Head, Host Interface	Yes	Yes	User	Uses MEKey

Name of Service	Service Description	Available on:	Available in FIPS mode	Available in non-FIPS mode	Role	Access to Keys/CSPs
Create Dump	Creates an encrypted diagnostic dump file and saves it to EEPROM. Afterwards, the ETD performs an Initial Program Load (IPL).	RJ45 (Ethernet)	Yes	Yes	C.O.	Uses and Modifies CTR_DRBG; Generates and Uses DEKey; Uses DEPubKey
Establish TLS Session	Establishes a TLS 1.0 (Transport Layer Security) session between the ETD and a KMS 2.x cluster.	RJ45 (Ethernet)	Yes	Yes	User	Uses and Modifies CTR_DRBG; Generates TLS_PM; Derives TLS_MS, TLS_EMK, TLS_DMK, TLS_ECK, TLS_DCK; Uses CA_Cert; Uses TDPubKey; Uses TDPrivKey
Export AKWK	Exports the AES Key Wrap Key (AKWK) to the KMS 2.x cluster, protected with RSA Encryption.	RJ45 (Ethernet)	Yes	Yes	User	Uses and Writes CTR_DRBG; Generates AKWK; Uses KWKPublicKey; Uses TLS_EMK; Uses TLS_ECK;
Input KWKPublicKey	Inputs the KWKPublicKey from a KMS 2.x cluster into the ETD.	RJ45 (Ethernet)	Yes	Yes	User	Writes KWKPublicKey; Uses TLS_DMK; Uses TLS_DCK

Name of Service	Service Description	Available on:	Available in FIPS mode	Available in non-FIPS mode	Role	Access to Keys/CSPs
Input ME_Key from KMS 2.x	Inputs one or more ME_Keys (protected with AES Key Wrap) into the ETD from the KMS 2.x cluster.	RJ45 (Ethernet)	Yes	Yes	User	Writes ME_Key; Uses TLS_DMK; Uses TLS_DCK; Uses AKWK;
ETD Configuration	Allows configuration of the ETD.	RJ45 (Ethernet)	Yes	Yes	C.O.	Not Applicable
Initial Program Load (IPL)	Causes tape drive to reinitialize and perform Power-Up Self-Tests.	RJ45 (Ethernet)	Yes	Yes	C.O.	Not Applicable
Audit Log	Allows the viewing, downloading, deletion of the ETD Audit Log.	RJ45 (Ethernet)	Yes	Yes	C.O.	Not Applicable
View Drive Data	Allows read access to ETD configuration data.	RJ45 (Ethernet)	Yes	Yes	C.O.	Not Applicable
Error Log	Allows the viewing, downloading, deletion of the ETD Error Log.	RJ45 (Ethernet)	Yes	Yes	C.O.	Not Applicable
Delete Dump	Deletes a dump file currently stored on the ETD.	RJ45 (Ethernet)	Yes	Yes	C.O.	Not Applicable

Name of Service	Service Description	Available on:	Available in FIPS mode	Available in non-FIPS mode	Role	Access to Keys/CSPs
Delete Perms	Deletes errors currently stored on ETD.	RJ45 (Ethernet)	Yes	Yes	C.O.	Not Applicable
Tape Management	Loads and/or Unloads a tape cartridge.	RJ45 (Ethernet)	Yes	Yes	C.O.	Not Applicable
Run Diagnostics	Perform ETD Diagnostics.	RJ45 (Ethernet)	Yes	Yes	C.O.	Not Applicable

Access Type Definitions:

Use: The CSP is used within an ETD security function or authentication mechanism.

Write: The CSP is written to internal volatile or persistent memory of the ETD. This is done during the input of a new CSP or the modification of an existing.

Generates: Generates the CSP using the FIPS Approved SP800-90 DRBG.

Derives: The CSP is derived using the Allowed TLS1.0 Key Derivation Function.

The ETD supports the unauthenticated services listed below in Table 7. None of the services modify, disclose, or substitute cryptographic keys and CSPs, or otherwise affect the security of the ETD.

Table 7: No Role Services

The following services are not associated with a specific role.

Name of Service	Service Description	Available On:
Show Status	Provides the current status of the ETD.	Drive Status LED, Encryption Status LED, Operator Panel, RJ45(Ethernet), Host Interface, DB15(RS232)

Name of Service	Service Description	Available On:
Power-Cycle/Perform Self-Tests	When the ETD is power-cycled, the ETD exercises the cryptographic hardware and firmware tests for the FIPS Approved algorithms, as listed in Section 9.1 .	Power Interface
Fibre Channel Interface Management	Provides non-security relevant ETD management and status output (see [ETDIM]).	Host Interface
Library Management	Provides non-security relevant ETD management and status output of the ETD.	DB15 (RS232)
Operator Panel	Provides non-security relevant ETD management and status output. See [ETDOG] for details.	Operator Panel

8 Operational Environment (Area 6)

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the ETD functions in a limited operational environment. As such, the module performs a firmware load test (RSA signature verification) to verify the authenticity and integrity of any newly loaded code (Note: New code images running on the hardware platform must be FIPS 140-2 validated as a single module).

9 Security Rules

9.1 FIPS 140-2 Security Requirements

This section documents the security rules enforced by the ETD cryptographic module.

- 1) The cryptographic module shall provide two distinct operator roles. These are the User role and the Crypto-Officer role.
- 2) When the module has not been placed in a valid role, the operator does not have access to any cryptographic services.
- 3) The cryptographic module shall encrypt and decrypt sensitive data using the AES-256 CCM algorithm.
- 4) The cryptographic module shall perform the following tests:
 - a) Power-up Self-tests
 - i) Cryptographic algorithm tests:
 - (1) AES ECB KAT (Encrypt/Decrypt)
 - (2) AES Key Wrap KAT (Wrap/Unwrap)

- (3) AES CBC (Encrypt/Decrypt)
- (4) AES CCM Firmware Implementation KAT (Encrypt/Decrypt)
- (5) AES CCM Hardware Implementation KAT (Encrypt/Decrypt)
- (6) SP800-90 CTR DRBG KAT
- (7) SHA-1 KAT
- (8) HMAC SHA-1 KAT
- (9) HMAC SHA-1(TLS) KAT (SHA-1 as used within this HMAC is tested as part of this KAT)
- (10) RSASSA-PKCS1-v1_5 Known Answer Test
 - ii) Firmware Integrity Test (32 bit CRC)
 - iii) CRC check on the keys (32 bit CRC)
- b) Conditional Self-tests:
 - i) Firmware Load Test: 2048 bit RSA PKCS1 digital signature verification
 - ii) SP800-90 DRBG Continuous Test
 - iii) NDRNG Continuous Test
- 5) An operator may command the module to perform the power up self-test by initiating a power cycle of the module.
- 6) The cryptographic module inhibits data output during self-tests, zeroization, key generation and error states.
- 7) Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
- 8) The module supports concurrent operators.

The operator can determine whether the power-on self-tests tests have passed or failed by observing the Operator Panel (See [ETDOG], Table 2-1 “Operator Panel Indicators”). If the Power Indicator is solid green, then all the power-on self tests have completed successfully. If a power-on self-test fails, then the Power Indicator LED will continue to flash, and the ETD will report an error and collect dump data, which includes turning on the Service Indicator LED (either flashing or solid).

10 Physical Security

10.1 Physical Security Mechanisms

The ETD multi-chip standalone cryptographic module includes the following physical security mechanisms:

- Production-grade components
- Production-grade metal enclosure

NOTE: The security stickers on the ETD do not provide FIPS-approved security.

11 Mitigation of Other Attacks Policy

The module has not been designed to mitigate any specific attacks.

12 References

Oracle Corp operator guides for T10000C Download Site.

<http://download.oracle.com/docs/cd/E19446-01/index.html>

[1619.1] IEEE Std 1619.1-2007, IEEE Standard for Authenticated Encryption with Length Expansion for Storage Devices. May 2008.

[CCM] NIST Special Publication 800-38C, *Recommendation for Block Modes of Operation: The CCM Mode for Authentication and Confidentiality*. U.S. DoC/NIST, May 2004. Available at <http://csrc.nist.gov/publications/nistpubs/index.html>

[ETDIM] StorageTek T10000 Tape Drive: Fibre Channel Interface Reference Manual (Part Number E20425-0, January 2011).

Available at http://download.oracle.com/docs/cd/E19446-01/en/E20425/E20425_01.pdf

[ETDOG] StorageTek T10000 Tape Drive Operator's Guide (Part Number E20714-01 , January 2011).

Available at: http://download.oracle.com/docs/cd/E19446-01/en/E20714/E20714_01.pdf

[FC-SB-3] Fibre Channel Single-Byte Command Code Sets-3 Mapping Protocol (FC-SB-3), Revision 1.6 specification.

[KMS2IM] Oracle Key Manager Administration Guide, November 2010, revision AA, Available at: <http://download.oracle.com/docs/cd/E19540-01/31619506Admin/31619506Admin.pdf>

[SPC-3] SCSI Primary Commands-3 (SPC-3)

[SSC-3] SCSI Stream Commands (SSC-3)

[TLS1.0] [RFC 2246](#): "The TLS Protocol Version 1.0".

June 2011

StorageTek™ T10000C Tape Drive Security Policy

[VOPUG] StorageTek Virtual Operator Panel User's Guide (Customer Version)
Part Number 20750-01, January 2011

Available at http://download.oracle.com/docs/cd/E19446-01/en/E20750/E20750_01.pdf

13 Definitions and Acronyms

AES	Advanced Encryption Standard
CO	Crypto-Officer
Data-At-Rest	Data that is stored on non-network attached media. Data-At-Rest in the context of the EDRS system is data stored on magnetic tape.
EDRS	Encrypted Data at Rest Solution
ETD	The Oracle Sun StorageTek T10000C Encrypting Tape Drive.
IPL	Initial Program Load. The process that brings up the ETD after a power-on or reset.
KMA	Key Management Appliance
KMS	Key Management System, which consists of two or more KMAs.
TLS	Transport Layer Security, v1.0, as defined by IETF RFC 2246
User Data	Arbitrary data which is being written to or read from magnetic tape.
VOP	Virtual Operator Panel – Software used to configure the ETD