Oracle StorageTek T10000D Tape Drive

FIPS 140-2 – Level 1 Validation
Non-Proprietary Security Policy

Hardware Part #: 7042136, 7314405

Firmware Version
RB411111

Security Policy Revision 0.12

Title: Oracle StorageTek T10000D FIPS 140-2 Security Policy
01.20.2017 **Author:** Acumen Security, LLC
Contributing Authors: Oracle

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.
Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com

Oracle is committed to developing practices and products that help protect the environment

Copyright © 2017, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. Oracle specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may reproduced or distributed whole and intact including this copyright notice.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Hardware and Software, Engineered to Work Together

© Copyright 2017 Oracle Corporation

This document may be freely reproduced and distributed whole and intact including this Copyright notice.

ORACLE

Table of Contents

© Copyright 2017 Oracle Corporation

This document may be freely reproduced and distributed whole and intact including this Copyright notice.

List of Figures

List of Tables

© Copyright 2017 Oracle Corporation

This document may be freely reproduced and distributed whole and intact including this Copyright notice.

© Copyright 2017 Oracle Corporation

This document may be freely reproduced and distributed whole and intact including this Copyright notice.

INTRODUCTION

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the StorageTek T10000D Tape Drive from Oracle Corporation. This Security Policy describes how the StorageTek T10000D 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 (CSE) 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 T10000D 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

[1] ETD – Encrypting Tape Drive

© Copyright 2017 Oracle Corporation

This document may be freely reproduced and distributed whole and intact including this Copyright notice.

- Finite State Machine
- Other supporting documentation as additional references

This Security Policy and the other validation submission documentation were produced by Acumen Security 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.

© Copyright 2017 Oracle Corporation

This document may be freely reproduced and distributed whole and intact including this Copyright notice.

2 STORAGETEK T10000D TAPE DRIVE

2.1 Module Overview

Oracle's StorageTek T10000D Tape Drive (Hardware Part #: 7042136/7314405; Firmware Version: RB411111) blends the highest capacity, performance, reliability, and data security to support demanding, 24/7 data center operations. The T10000D delivers fast write speeds (252 MB[2]/sec[3]) to a native 8.5 TB of magnetic tape storage; making it ideal for data center operations with growing data volume. The T10000D provides data protection with built-in AES[4] hardware encryption and multiple FIPS 140-2 Approved modes of operation. Customers can be assured that their data will always be secure, in any of these FIPS 140-2 Approved modes. The T10000D encrypting tape drive (ETD) 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 mixed mode of operation supporting both FIPS 140-2 Approved and non-FIPS 140-2 Approved operations is also available. This mode of operation provides a non FIPS-140-2 Approved method for encrypting the tape cartridge contents for customers who do not require FIPS 140 protected content.

The StorageTek T10000D Tape Drive is featured in Figure 1 below.

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

© Copyright 2017 Oracle Corporation

This document may be freely reproduced and distributed whole and intact including this Copyright notice.

Figure 1 – StorageTek T10000D Tape Drive

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[5] 1.0.

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 T10000D 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 T10000D 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 modes of operation. Connections to the ETD from the VOP are provided through the Telnet and SSH network protocols.

2.1.3 StorageTek T10000D Tape Drive Deployment

A sample deployment scenario for the StorageTek T10000D Tape Drive with encryption enabled is provided in Figure 2 below. The ETD is shown with a red, dotted line surrounding it, representing its cryptographic boundary.

[5] TLS – Transport Layer Security

© Copyright 2017 Oracle Corporation

This document may be freely reproduced and distributed whole and intact including this Copyright notice.

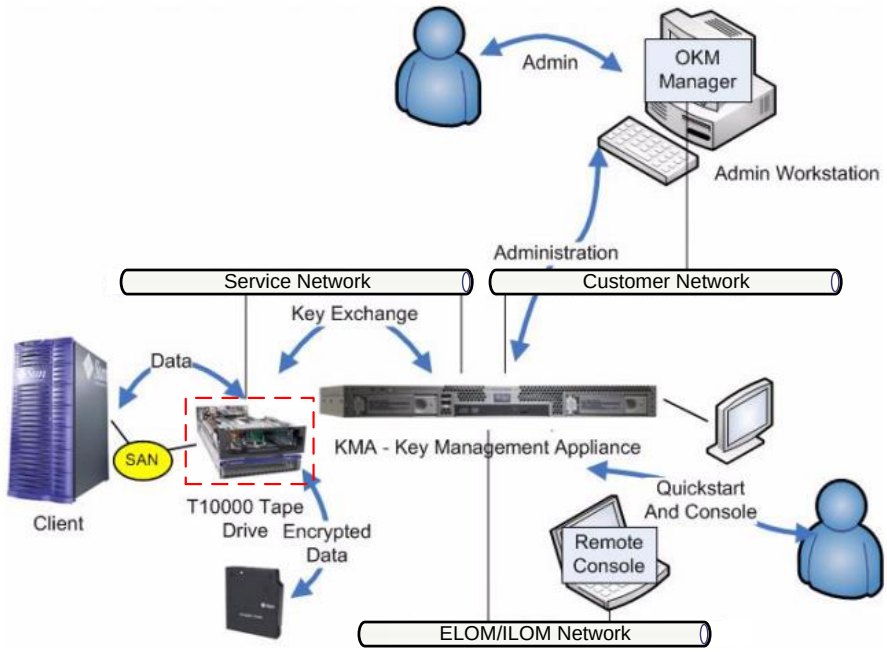

Figure 2 – StorageTek T10000D Tape Drive Deployment Scenario

© Copyright 2017 Oracle Corporation

This document may be freely reproduced and distributed whole and intact including this Copyright notice.

2.2 Module Specification

The StorageTek T10000D Tape Drive is validated at the FIPS 140-2 section levels shown in Table 1 for all 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[6]	1
9	Self-tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A

The StorageTek T10000D 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 T10000D Tape Drive is defined by the tape drive's commercial-grade, metallic enclosure.

The module provides several 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 Mixed mode of operation. Each of the Approved modes and the Mixed 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 T10000D Tape Drive. This mode provides secure encryption and decryption of data stored on magnetic tape, using the 256-bit AES cryptographic algorithm. While

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

© Copyright 2017 Oracle Corporation

This document may be freely reproduced and distributed whole and intact including this Copyright notice.

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". In addition, the operator shall verify that the "Use OKM or DPKM[7]" label is set to "OKM". 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 magnetic tape. Encryption and decryption are performed using the 256-bit 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 mode and the Mixed 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". Finally, the operator shall confirm that the "Use OKM or DPKM" label is set to "OKM". 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

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 Mixed mode while operating the module in the Encryption Disabled Mode.

[7] DPKM – Data Path Key Management

© Copyright 2017 Oracle Corporation

This document may be freely reproduced and distributed whole and intact including this Copyright notice.

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". Finally, the operator shall confirm that the "Use OKM or DPKM" label is set to "UNKN[8]". 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 Mixed Mode

The StorageTek T10000D Tape Drive is capable of operating in a Mixed mode of operation. The Mixed mode of operation is defined as a mode of operation that allows both FIPS approved and non-approved services. Mixed mode of operation supports the following approved services, SSH and firmware update. No other cryptographic services are considered approved in Mixed mode.

Mixed mode of operation supports non-approved key import and export (in plaintext). These methods of key import and export provide no cryptographic security. Any data encrypted with this keying material is considered plaintext.

Mixed mode is entered when DPKM is enabled through the VOP. DPKM allows an operator to use the SCSI[9] commands `SPIN` and `SPOUT` in order to import and export keying material to and from the module in plaintext.

Keys and CSPs established in any of the other Approved modes are zeroized prior to operating in the Mixed mode. Additionally, keys and CSPs established in Mixed Mode are zeroized prior to operating in the any of the other Approved modes. An operator of the module can determine if the module is operating in the Mixed mode by using the VOP to confirm that the "Use OKM or DPKM" label is set to "DPKM". Instructions to place the module into the Mixed are provided in Section 3.1.5. An operator will be able to switch to the Encryption Disabled Mode while operating the module in the Mixed Mode.

2.3 Module Interfaces

The following is a list of the FIPS 140-2 logical interfaces supported by the StorageTek T10000D Tape Drive:

- Data Input
- Data Output

[8] UNKN - Unknown
[9] SCSI – Small Computer System Interface

© Copyright 2017 Oracle Corporation

This document may be freely reproduced and distributed whole and intact including this Copyright notice.

- Control Input
- Status Output

Additionally, the module supports a Power Input interface.

2.3.1 FIPS 140-2 Logical Interface Mapping

Figure 3 shows the front of the StorageTek T10000D Tape Drive. The opening provides an entryway for an approved StorageTek T10000 T1 or T2 Tape Cartridge. The ETD will not operate if the wrong tape cartridge is inserted. This entryway provides the Tape Head and RFID[10] 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.

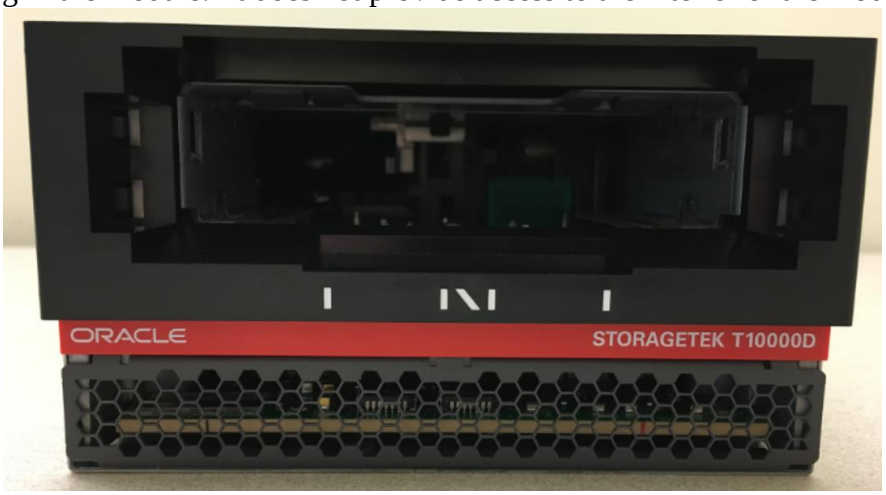

Figure 3 - StorageTek T10000D Tape Drive (Front)

Figure 4 shows the rear of the StorageTek T10000D Tape Drive. It provides the following physical interfaces:

- Tape Transport Interface (TTI) – RS-232[11] Serial connection
- Power Supply Connector
- Host Interfaces – Fibre Channel connection (Hardware version # 7042136)/iSER connection (Hardware version # 7314405)
- Recessed Switch
- Ethernet Port – RJ45[12] connection

[10] RFID – Radio Frequency Identification
[11] RS-232 – Recommended Standard 232
[12] RJ45 – Registered Jack 45

© Copyright 2017 Oracle Corporation

This document may be freely reproduced and distributed whole and intact including this Copyright notice.

Figure 4 - StorageTek T10000D Tape Drive (Rear)

The bottom of the StorageTek T10000D Tape Drive (Figure 5) 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.

*The additional port pictured is the Manufacturing Servo Interface. This interface is not operational in any of the modes of operation; therefore, it is not listed in the interfaces table (Table 2) below.

© Copyright 2017 Oracle Corporation

This document may be freely reproduced and distributed whole and intact including this Copyright notice.

Figure 5 – StorageTek T10000D Tape Drive (Bottom)[13]

Table 2 provides a mapping of all of the physical interfaces of the StorageTek T10000D 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.

[13] The security seal shown does not provide additional physical security

© Copyright 2017 Oracle Corporation

This document may be freely reproduced and distributed whole and intact including this Copyright notice.

Table 2 – Mapping of FIPS 140-2 Logical Interfaces to StorageTek T10000D 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)
TTI connector (RS-232)	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[14] address to the default IP address (10.0.0.1) Long press: Force ETD data dump[15]
Power supply connector	1	Power	100-240 VAC[16] @ 50-60 Hz[17]

[14] IP – Internet Protocol
[15] All unencrypted dumps shall be deleted by the CO after their creation
[16] VAC – Volts Alternating Current
[17] Hz - Hertz

© Copyright 2017 Oracle Corporation

This document may be freely reproduced and distributed whole and intact including this Copyright notice.

Physical Interface	Quantity	FIPS 140-2 Logical Interfaces Supported	Description
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. On hardware version 7042136 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[18], in accordance with the Fibre Channel Single-Byte Command Code Sets-3 Mapping Protocol (FC-SB-3), Revision 1.6 specification 3) On hardware version 7314405 the interface supports iSCSI[19] Extensions for RDMA[20] (iSER) version 1.0, July 2003
Ethernet Port (RJ-45)	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[21] server.

[18] FICON – Fibre connection
[19] iSCSI – Internet Small Computer System Interface
[20] RDMA – Remote Direct Memory Access
[21] SNMP – Simple Network Management Protocol

© Copyright 2017 Oracle Corporation

This document may be freely reproduced and distributed whole and intact including this Copyright notice.

Physical Interface	Quantity	FIPS 140-2 Logical Interfaces Supported	Description
Operator Panel Port[22]	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[23] display output interface. The LCD is used to display ETD status and configuration menu text. C. Four switch signals (input): 1. IPL[24] 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 T10000D Tape Drive VOP Status Information

The module outputs status information via the Ethernet Port to the VOP to provide a more detailed drive and encryption status to the operator. Drive statuses include whether the ETD has a tape, is online, or has encountered an error. Encryption statuses include whether the ETD has correct encryption keys and if it is capable of performing encryption. Detailed statuses of the module are provided in the *StorageTek Virtual Operator Panel User's Guide*; freely available at: http://docs.oracle.com.

[22] Status and control information provided through Operator Panel Port is provided in Chapter 2 of the *StorageTek T10000 Tape Drive Operator's Guide.*
[23] LCD – Liquid Crystal Display
[24] IPL – Initial Program Load

© Copyright 2017 Oracle Corporation

This document may be freely reproduced and distributed whole and intact including this Copyright notice.

2.4 Roles and Services

The StorageTek T10000D 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 twelve concurrent operators. Each connection to the ETD is logically separated by the module by unique session keys.

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.
- 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 T10000D Tape Drive which includes placing the module into one of the modes of operations. A list of services available to the CO, and the Approved mode the service is available in, is provided in Table 3.

© Copyright 2017 Oracle Corporation

This document may be freely reproduced and distributed whole and intact including this Copyright notice.

Table 3 – 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 Mixed Mode	CA_Cert – WX TDPrivKey – W TDPubKey – W
Enable Mixed Mode	Bring the module into a Mixed mode of operation	Encryption Disabled	None
Configure Module	Perform routine module configuration	Permanent Encryption Encryption Enabled Encryption Disabled Mixed Mode	None
Place drive online/offline	Add or remove Fibre Channel and iSER connectivity to the ETD	Permanent Encryption Encryption Enabled Encryption Disabled Mixed Mode	None
Load Firmware	Update module firmware	Permanent Encryption Encryption Enabled Encryption Disabled Mixed Mode	FSPubKey – RX FSRootCert – X
Reset	Zeroization of all keys and CSPs	Permanent Encryption Encryption Enabled Encryption Disabled Mixed Mode	All Keys and CSPs[25] – W
Access Module via Virtual Operator's Panel (VOP)	Log into VOP and manage the module	Permanent Encryption Encryption Enabled Encryption Disabled Mixed Mode	None
Create Dump (Encrypted)	Create an encrypted dump file and save to EEPROM[26]	Permanent Encryption Encryption Enabled	DRBG[27] 'Key' Value – WRX DRBG 'V' Value – WRX DRBG Seed – WRX DEKey – WX DEPubKey – X

[25] Dump excludes DEPubKey, FSPubKey, and FSRootCert
[26] EEPROM – Electronically Erasable Programmable Read-Only Memory
[27] DRBG – Deterministic Random Bit Generator

© Copyright 2017 Oracle Corporation

This document may be freely reproduced and distributed whole and intact including this Copyright notice.

Service	Description	Approved Mode	CSP and Type of Access
Create Dump (Unencrypted)	Create an unencrypted dump file and save to EEPROM	Permanent Encryption Encryption Enabled Encryption Disabled Mixed Mode	None
Initial Program Load (IPL)	Reinitialize module and run self-tests	Permanent Encryption Encryption Enabled Encryption Disabled Mixed Mode	None
Download Audit Log	Downloadaudit log	Permanent Encryption Encryption Enabled Encryption Disabled Mixed Mode	None
View Drive Data	Read module configuration data	Permanent Encryption Encryption Enabled Encryption Disabled Mixed Mode	None
Download event logs	Download the currently stored event logs	Permanent Encryption Encryption Enabled Encryption Disabled Mixed Mode	None
Download Dump	Download the currently stored dump file.	Permanent Encryption Encryption Enabled Encryption Disabled Mixed Mode	None
Download Perm logs	Download the currently stored permanent error logs	Permanent Encryption Encryption Enabled Encryption Disabled Mixed Mode	None
Delete Event Logs	Delete the currently stored event logs.	Permanent Encryption Encryption Enabled Encryption Disabled Mixed Mode	None
Delete Dump	Delete the currently stored dump file	Permanent Encryption Encryption Enabled Encryption Disabled Mixed Mode	None
Delete Perm Logs	Deletes currently stored permanent error logs	Permanent Encryption Encryption Enabled Encryption Disabled Mixed Mode	None

© Copyright 2017 Oracle Corporation

This document may be freely reproduced and distributed whole and intact including this Copyright notice.

Service	Description	Approved Mode	CSP and Type of Access
Tape Management	Load or unload a new tape cartridge into the module	Permanent Encryption Encryption Enabled Encryption Disabled Mixed Mode	None
Run Diagnostics	Perform a diagnostic test on the module	Permanent Encryption Encryption Enabled Encryption Disabled Mixed Mode	None

2.4.2 Non-Approved Services available in Mixed Mode

DPKM and the `SPIN` and `SPOUT` SCSI commands available in Mixed mode of operation are considered non-approved services and do not provide any FIPS-approved cryptographic protection. Because `SPIN` and `SPOUT` are considered a plaintext key establishment technique, they shall not be used in the Approved mode of operation. Any keys established by `SPIN` or `SPOUT` are considered non-Approved keys and shall not be used in the Approved mode of operation.

2.4.3 User Role

The User of the StorageTek T10000D 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 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 4.

Table 4 – 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 Mixed Mode	None
Read Plaintext Data	Read plaintext data from the tape cartridge	Permanent Encryption Encryption Enabled Encryption Disabled Mixed Mode	None

© Copyright 2017 Oracle Corporation

This document may be freely reproduced and distributed whole and intact including this Copyright notice.

Establish TLS Session	Establish connection with OKM cluster	Permanent Encryption Encryption Enabled	DRBG 'Key' Value – WRX DRBG 'V' Value – WRX DRBG Seed – WRX TLS_PM – WRX TLS_MS – WRX TLS_EMK – W TLS_DMK – W TLS_ECK – W TLS_DCK – W CA_Cert – X TDPubKey – X TDPrivKey – X
Establish SSH session	Establish connection with remote workstation	Permanent Encryption Encryption Enabled Encryption Disabled Mixed Mode	SSH_HOST_PRIV – X SSH_HOST_PUB - X SSH_SK - WRX SSH_SA - WRX SSH_KEX_PRI - WRX
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

2.4.4 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 5 lists the services available to operators not required to assume an authorized role. These services are available in all Approved modes of operation.

© Copyright 2017 Oracle Corporation

This document may be freely reproduced and distributed whole and intact including this Copyright notice.

Table 5 – Additional Operator Services

Service	Description	Approved Mode	CSP and Type of Access
Show Status	Determine the current status of the module by reading the information provided on the VOP	Permanent Encryption Encryption Enabled Encryption Disabled Mixed Mode	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 Mixed Mode	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 Mixed Mode	None
Interface Port Management	Manage the module through the Interface Port (non-security relevant)	Permanent Encryption Encryption Enabled Encryption Disabled Mixed Mode	None
Library Management	Manage the module and retrieve status information through the TTI (non-security relevant)	Permanent Encryption Encryption Enabled Encryption Disabled Mixed Mode	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 Mixed Mode	None

2.4.5 Additional StorageTek T10000D Tape Drive Services

In addition to the services provided in the sections above, the StorageTek T10000D Tape Drive provides additional services to operators which do not affect the overall security of the module. These additional, non-security relevant services are listed in the documents stated in Section 3 (Secure Operation) of this Security Policy. These documents are freely available at http://docs.oracle.com.

2.5 Physical Security

The StorageTek T10000D 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.

© Copyright 2017 Oracle Corporation

This document may be freely reproduced and distributed whole and intact including this Copyright notice.

NOTE: The labels pictured in Figure 5 above do not add any additional security to the module.

2.6 Operational Environment

The operational environment for the StorageTek T10000D Tape Drive consists of two NIOS II processors, which are the module's only general-purpose processors. These processors execute the module's firmware (Firmware Version: RB411111).

New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into this module is out of the scope of this validation and require a separate FIPS 140-2 validation.

The module does not employ a general purpose Operating System.

2.7 Cryptographic Key Management

The StorageTek T10000D Tape Drive was designed to operate in several FIPS-Approved modes of operation: Permanent Encryption Mode, Encryption Enabled Mode, Encryption Disabled Mode, and Mixed 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 T10000D 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 inTable 6.

Table 6 – FIPS-Approved Algorithms in StorageTek T10000D Tape Drive (Permanent Encryption and Encryption Enabled Modes)

Algorithm	Implementation Description	Certificate Number
AES[28] 256-bit ECB[29] mode	Provides encryption for multiple services including AES in ECB mode as used in firmware AES CCM encryption (with Cert # 4039) and with the SP[30] 800-90A CTR[31] DRBG (Cert # 1209)	4039

[28] AES – Advanced Encryption System
[29] ECB – Electronic Code Book
[30] SP – Special Publication
[31] CTR - Counter

© Copyright 2017 Oracle Corporation

This document may be freely reproduced and distributed whole and intact including this Copyright notice.

Algorithm	Implementation Description	Certificate Number
AES 256-bit ECB mode (Used with OKM)	Provides AES in ECB mode as used to unwrap AES Media Keys[32] being sent from the OKM. (Cert # 4047)	4047
AES Key Wrap 256-bit (Used with OKM)	Unwrap AES Media Keys being sent from the OKM (Used with AES ECB Cert #4047)	4047
AES 256-bit CCM mode	AES in CCM mode as used with AES in ECB mode with Cert # 4039	4039
AES 128-bit CTR mode	AES in CTR mode (with AES-ECB-128 as the forward cipher funtion) used in remote SSH sessions.	4039
AES 128-bit CBC mode	AES in CBC mode used in remote SSH sessions.	4039
AES 256-bit CBC[33]mode (TLS 1.0/1.1 implementation)	AES in CBC mode used in a TLS session between the ETD and OKM	4040
AES 256-bit ECB mode (DCCM hardware implementation)	AES in ECB mode as used in hardware AES CCM encryption with Cert # 2760	2760
AES 256-bit CCM mode (DCCM hardware implementation)	AES in CCM mode as used with AES in ECB mode Cert # 2760	2760
SHA[34]-1	Provides hashing for multiple services including, digital signature verification (Used with HMAC SHA-1 (Cert # 2636), RSA 2048-bit (Cert # 2074)); User data hashing; Used as part of the SSH KDF (Cert #866).	3330
SHA-1 (TLS 1.0/1.1 implementation)	Used as part of the TLS 1.0/1.1 Key Derivation Function; Used with HMAC SHA-1 (TLS 1.0/1.1 implementation Cert # 867).	3331
SHA-256	Provides hashing for multiple services including, digital signature verification (Used with RSA 2048 (Cert # 2074)) and as part of the SSH Key Derivation Function) (Used with Cert #866). SHA-256 is also used with RSA 2048 Signature Generation and ECDSA Signature Generation (Cert #905).	3330
HMAC[35] SHA-1 (TLS 1.0/1.1 implementation)	Provides integrity during a TLS session; Used with SHA-1 (Cert #: 3331)	2637
HMAC SHA-1	Provides integrity during a SSH session; Used with SHA-1 (Cert #3330)	2636

[32] Media Keys are a defined CSP. See Table 9 in VE07.03.01
[33] CBC – Cipher Block Chaining
[34] SHA – Secure Hash Algorithm
[35] HMAC – (Keyed-) Message Authentication Code

© Copyright 2017 Oracle Corporation

This document may be freely reproduced and distributed whole and intact including this Copyright notice.

Algorithm	Implementation Description	Certificate Number
HMAC SHA-1 (OKM Agent implementation)	Provide keyed message authentication when creating the challenge responses as part of the certificate service of the OKM. Used with SHA-1 (Cert # 3330)	2642
RSA 2048-bit PKCS[36] #1 v1.5 Signature Verification	Verifies the signature of a new firmware image to be loaded onto the ETD; Used with SHA-256 (Cert # 3330)	2074
RSA 2048-bit PKCS #1 v1.5 Signature Generation	Performs session establishment in support of SSH.	2074
RSA 2048-bit FIPS 186-4 Key Generation	Performs Key Generation in support of SSH	2074
Elliptic-Curve P-256 (ECDSA) Key Pair Generation	Performs Key Generation in support of SSH with NIST curve P-256	905
Elliptic-Curve P-256(ECDSA) Signature Generation	Performs session establishment in support of SSH, with NIST curve P-256	905
TLS 1.0 and 1.1 Key Derivation Note: The TLS protocol has not been reviewed or tested by the CAVP and CMVP	TLS 1.0 and 1.1 Key Derivation (SP800-135 rev1; Section 4.2.1); Used with SHA-1 (Cert # 3331) and DRBG (Cert # 1209)	867
SSH Key Derivation Note: The SSH protocol has not been reviewed or tested by the CAVP and CMVP	SSH Key Derivation (SP800-135 rev1; Section 5.2)	866
SP800-90A CTR DRBG	Generates random numbers for nonces and keys for multiple services including TLS, SSH, and OKM	1209

2.7.2 Encryption Disabled Cryptographic Algorithm Implementations

The Encryption Disabled Approved Mode utilizes a subset of the cryptographic algorithms listed in Table 6. A list of cryptographic algorithms used by the module while operating in the Encryption Disabled Mode is provided as Table 7.

Table 7 – FIPS-Approved Algorithms in StorageTek T10000D Tape Drive (Encryption Disabled Mode)

Algorithm	Implementation Description	Certificate Number
AES[37] 256-bit ECB[38] mode	Provides encryption for multiple services including with the SP[39] 800-90A CTR[40] DRBG (Cert # 1209)	4039

[36] PKCS – Public Key Cryptographic Standard
[37] AES – Advanced Encryption System
[38] ECB – Electronic Code Book
[39] SP – Special Publication

© Copyright 2017 Oracle Corporation

This document may be freely reproduced and distributed whole and intact including this Copyright notice.

Algorithm	Implementation Description	Certificate Number
AES 128-bit CTR mode	AES in CTR mode used in remote SSH sessions.	4039
AES 128-bit CBC mode	AES in CBC mode used in remote SSH sessions.	4039
SHA[41]-1	Provides hashing for multiple services including, digital signature verification (Used with HMAC SHA-1 (Cert # 2636), RSA 2048-bit (Cert # 2074)); User data hashing; Used as part of the SSH KDF (Cert #866).	3330
SHA-256	Provides hashing for multiple services including, digital signature verification (Used with RSA 2048 (Cert # 2074)) and as part of the SSH Key Derivation Function (Used with Cert #866). SHA-256 is also used with RSA 2048 Signature Generation and ECDSA Signature Generation (Cert #905).	3330
HMAC SHA-1	Provides integrity during a SSH session; Used with SHA-1 (Cert # 3330)	2636
RSA 2048-bit PKCS[42] #1 v1.5 Signature Verification	Verifies the signature of a new firmware image to be loaded onto the ETD; Used with SHA-1 (Cert #3330) and SHA-256 (Cert # 3330)	2074
RSA 2048-bit PKCS #1 v1.5 Signature Generation	Performs session establishment in support of SSH.	2074
RSA 2048-bit FIPS 186-4 Key Generation	Performs Key Generation in support of SSH	2074
Elliptic-Curve P-256 Key Pair Generation	Performs Key Generation in support of SSH with NIST curve P-256	905
Elliptic-Curve P-256 DSA (ECDSA)	Performs session establishment in support of SSH, with NIST curve P-256	905
SSH Key Derivation Note: The SSH protocol has not been reviewed or tested by the CAVP and CMVP	SSH Key Derivation (SP800-135 rev1; Section 5.2)	866
SP800-90A CTR DRBG	Generates random numbers for nonces and keys for multiple services including SSH	1209

[40] CTR - Counter
[41] SHA – Secure Hash Algorithm
[42] PKCS – Public Key Cryptographic Standard

© Copyright 2017 Oracle Corporation

This document may be freely reproduced and distributed whole and intact including this Copyright notice.

2.7.3 Mixed Mode Algorithm Implementations

A list of cryptographic algorithms used by the module while operating in the Mixed Mode is provided in Table 8.

Table 8 – Mixed Mode Security Functions

Algorithm	Implementation Description	Certificate Number
AES[43] 256-bit ECB[44] mode	Provides encryption for multiple services including with the SP[45] 800-90A CTR[46] DRBG (Cert # 1209)	4039
AES 128-bit CTR mode	AES in CTR mode used in remote SSH sessions.	4039
AES 128-bit CBC mode	AES in CBC mode used in remote SSH sessions.	4039
SHA[47]-1	Provides hashing for multiple services including, digital signature verification (Used with HMAC SHA-1 (Cert # 2636), RSA 2048-bit (Cert # 2074)). Used as part o the SSH KDF (Cert #866).	3330
SHA-256	Provides hashing for multiple services including, digital signature verification (Used with RSA 2048 (Cert # 2074)) and as part of the SSH Key Derivation Function (Used with (Cert # 866)). SHA-256 is also used with RSA 2048 Signature Generation and ECDSA Signature Generation (Cert #905).	3330
HMAC SHA-1	Provides integrity during a SSH session; Used with SHA-1 (Cert # 3330)	2636
RSA 2048-bit PKCS[48] #1 v1.5 Signature Verification	Verifies the signature of a new firmware image to be loaded onto the ETD; Used with SHA-1 and SHA-256 (Cert # 3330)	2074
RSA 2048-bit PKCS #1 v1.5 Signature Generation	Performs session establishment in support of SSH.	2074
RSA 2048-bit FIPS 186-4 Key Generation	Performs Key Generation in support of SSH	2074

[43] AES – Advanced Encryption System
[44] ECB – Electronic Code Book
[45] SP – Special Publication
[46] CTR - Counter
[47] SHA – Secure Hash Algorithm
[48] PKCS – Public Key Cryptographic Standard

© Copyright 2017 Oracle Corporation

This document may be freely reproduced and distributed whole and intact including this Copyright notice.

Algorithm	Implementation Description	Certificate Number
Elliptic-Curve P-256 Key Pair Generation	Performs Key Generation in support of SSH with NIST curve P-256	905
Elliptic-Curve P-256 DSA (ECDSA)	Performs session establishment in support of SSH, with NIST curve P-256	905
SSH Key Derivation Note: The TLS protocol has not been reviewed or tested by the CAVP and CMVP	SSH Key Derivation (SP800-135 rev1; Section 5.2)	866
SP800-90A CTR DRBG	Generates random numbers for nonces and keys for multiple services including SSH	1209

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 receives data from an OKM cluster wrapped with AES Key Wrap. AES Key Wrap, as defined in SP 800-38F, is an approved key wrapping, key establishment methodology.

- AES (Cert #4047, 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)
- EC Diffie-Hellman (key agreement; key establishment methodology provides 128 bits of encryption strength)
- Diffie-Hellman (key agreement; 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 NDRNG provides a minimum of 384-bits to the DRBG for use in key generation.
- The module provides MD5 for use with TLS 1.0 protocol.

© Copyright 2017 Oracle Corporation

This document may be freely reproduced and distributed whole and intact including this Copyright notice.

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

- EC Diffie-Hellman (key agreement; key establishment methodology provides 128 bits of encryption strength)
- Diffie-Hellman (key agreement; 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 NDRNG provides a minimum of 384-bits to the DRBG for use in key generation.
- The module provides MD5 for use with TLS 1.0 protocol.

© Copyright 2017 Oracle Corporation

This document may be freely reproduced and distributed whole and intact including this Copyright notice.

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 9.

Table 9 – 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[49] and FPGA[50]	"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	Output encrypted via DEKey	Plaintext in EEPROM and RAM	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 and RAM	"Reset" service; Switch Approved Mode	Authenticate the module to OKM cluster appliance during TLS session

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

© Copyright 2017 Oracle Corporation

This document may be freely reproduced and distributed whole and intact including this Copyright notice.

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 1.0/1.1 session
TLS_MS	48 bytes pseudo-random data	Generated internally via TLS 1.0/1.1 PRF[51]	Output encrypted via DEKey	Plaintext in RAM	"Reset" service; Power cycle; Switch Approved Mode	Master secret for TLS 1.0/1.1 session
TLS_EMK	HMAC SHA-1 (112-bits)	Generated internally via TLS 1.0/1.1 PRF	Output encrypted via DEKey	Plaintext in RAM	"Reset" service; Power cycle; Switch Approved Mode	Authentication key for data leaving the module (per TLS 1.0/1.1)
TLS_DMK	HMAC SHA-1 (112-bits)	Generated internally via TLS 1.0/1.1 PRF	Output encrypted via DEKey	Plaintext in RAM	"Reset" service; Power cycle; Switch Approved Mode	Authentication key for data entering the module (per TLS 1.0/1.1)
TLS_ECK	AES CBC 256-bit	Generated internally via TLS 1.0/1.1 PRF	Output encrypted via DEKey	Plaintext in RAM	"Reset" service; Power cycle; Switch Approved Mode	Encryption key for data leaving the module (per TLS 1.0/1.1)
TLS_DCK	AES CBC 256-bit	Generated internally via TLS 1.0/1.1 PRF	Output encrypted via DEKey	Plaintext in RAM	"Reset" service; Power cycle; Switch Approved Mode	Decryption key for data entering the module (per TLS 1.0/1.1)
SSH_HOST_PRIV	RSA 2048-bit Private Key ECDSA P256 Curve Private Key	Generated internally via Approved DRBG	Output encrypted via DEKey	Plaintext in EEPROM	"Reset" service; Power cycle; Switch Approved Mode	SSH Authentication

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

© Copyright 2017 Oracle Corporation

This document may be freely reproduced and distributed whole and intact including this Copyright notice.

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
SSH_HOST_PUB	RSA 2048-bit Public Key ECDSA P256 Curve Public Key	Generated internally via Approved DRBG	Output plaintext	Plaintext in EEPROM	"Reset" service; Power cycle; Switch Approved Mode	SSH Authentication
SSH_SK	AES CTR 128-bit AES CBC 128-bit	Generated internally via SSH PRF	Output encrypted via DEKey	Plaintext in RAM	"Reset" service; Power cycle; Switch Approved Mode	SSH Session Keys (per SSH 2.0)
SSH_SA	HMAC SHA-1 (112-bits)	Generated internally via SSH PRF	Output encrypted via DEKey	Plaintext in RAM	"Reset" service; Power cycle; Switch Approved Mode	SSH Session integrity Keys (per SSH 2.0)
SSH_KEX_PRI	ECDH P-256 Curve (128-bits) or FFC DH Group 14 (112-bits)	Generated internally via ECDH or FFC DH	Output encrypted via DEKey	Plaintext in RAM	"Reset" service; Power cycle; Switch Approved Mode	SSH Key Exchange Private Key (per SSH 2.0)
SSH_KEX_PUB	ECDH P-256 Curve (128-bits) or FFC DH Group 14 (112-bits)	Generated internally via ECDH or FFC DH	Output encrypted via SSH_SK	Plaintext in RAM	Power cycle; Switch Approved Mode	SSH Key Exchange Public Key (per SSH 2.0)
CA_Cert	RSA 2048-bit public Key	Generated externally. Input in plaintext via CA[52]	Output encrypted via DEKey	Plaintext in EEPROM and RAM	"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 and RAM	"Reset" service; Switch Approved Mode	Wrap AKWK to be sent to OKM cluster

[52] CA – Certificate Authority

© Copyright 2017 Oracle Corporation

This document may be freely reproduced and distributed whole and intact including this Copyright notice.

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	Output encrypted via DEKey	Plaintext in EEPROM and RAM	Not Applicable	Verify the chain of certificates provided by the new firmware image
DRBG Seed	Random bit value	Generated internally	Output encrypted via DEKey	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	Output encrypted via DEKey	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	Output encrypted via DEKey	Plaintext in RAM	"Reset" service; Power cycle; Switch Approved Mode	Internal state value for the CTR_DRBG

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 10.

Table 10 – List of Cryptographic Keys, Cryptographic Key Components, and CSPs (Encryption Disabled Mode)

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use

© Copyright 2017 Oracle Corporation

This document may be freely reproduced and distributed whole and intact including this Copyright notice.

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	Output encrypted via SSH_SK	Plaintext in EEPROM and RAM	Not Applicable	Verify the chain of certificates provided by the new firmware image
SSH_HOST_PRIV	RSA 2048-bit Private Key ECDSA P256 Curve Private Key	Generated internally via Approved DRBG	Output encrypted via SSH_SK	Plaintext in EEPROM	"Reset" service; Power cycle; Switch Approved Mode	SSH Authentication
SSH_HOST_PUB	RSA 2048-bit Public Key ECDSA P256 Curve Public Key	Generated internally via Approved DRBG	Output plaintext	Plaintext in EEPROM	"Reset" service; Power cycle; Switch Approved Mode	SSH Authentication
SSH_SK	AES CTR 128-bit AES CBC 128-bit	Generated internally via SSH PRF	Output encrypted via SSH_SK	Plaintext in RAM	Power cycle; Switch Approved Mode	SSH Session Keys (per SSH 2.0)
SSH_SA	HMAC SHA-1 (112-bits)	Generated internally via SSH PRF	Output encrypted via SSH_SK	Plaintext in RAM	Power cycle; Switch Approved Mode	SSH Session Integrity Keys (per SSH 2.0)
SSH_KEX_PRI	ECDH P-256 Curve (128-bits) or FFC DH Group 14 (112-bits)	Generated internally via ECDH or FFC DH	Output encrypted via SSH_SK	Plaintext in RAM	Power cycle; Switch Approved Mode	SSH Key Exchange Private Key (per SSH 2.0)
SSH_KEX_PUB	ECDH P-256 Curve (128-bits) or FFC DH Group 14 (112-bits)	Generated internally via ECDH or FFC DH	Output encrypted via SSH_SK	Plaintext in RAM	Power cycle; Switch Approved Mode	SSH Key Exchange Public Key (per SSH 2.0)

© Copyright 2017 Oracle Corporation

This document may be freely reproduced and distributed whole and intact including this Copyright notice.

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
DRBG Seed	Random bit value	Generated internally	Output encrypted via DEKey	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	Output encrypted via DEKey	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	Output encrypted via DEKey	Plaintext in RAM	"Reset" service; Power cycle; Switch Approved Mode	Internal state value for the CTR_DRBG

2.7.6 Mixed Mode Cryptographic Keys and Critical Security Parameters

The cryptographic keys, key components, and other CSPs used by the module while operating in the Mixed Mode are shown in Table 11.

Table 11 – List of Cryptographic Keys, Cryptographic Key Components, and CSPs (Mixed 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	Output encrypted via SSH_SK	Plaintext in EEPROM and RAM	Not Applicable	Verify the chain of certificates provided by the new firmware image

© Copyright 2017 Oracle Corporation

This document may be freely reproduced and distributed whole and intact including this Copyright notice.

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
SSH_HOST_PRIV	RSA 2048-bit Private Key ECDSA P256 Curve Private Key	Generated internally via Approved DRBG	Output encrypted via SSH_SK	Plaintext in EEPROM	"Reset" service; Power cycle; Switch Approved Mode	SSH Authentication
SSH_HOST_PUB	RSA 2048-bit Public Key ECDSA P256 Curve Public Key	Generated internally via Approved DRBG	Output plaintext	Plaintext in EEPROM	"Reset" service; Power cycle; Switch Approved Mode	SSH Authentication
SSH_SK	AES CTR 128-bit AES CBC 128-bit	Generated internally via SSH PRF	Output encrypted via SSH_SK	Plaintext in RAM	Power cycle; Switch Approved Mode	SSH Session Keys (per SSH 2.0)
SSH_SA	HMAC SHA-1 (112-bits)	Generated internally via SSH PRF	Output encrypted via SSH_SK	Plaintext in RAM	Power cycle; Switch Approved Mode	SSH Session Integrity Keys (per SSH 2.0)
SSH_KEX_PRI	ECDH P-256 Curve (128-bits) or FFC DH Group 14 (112-bits)	Generated internally via ECDH or FFC DH	Output encrypted via SSH_SK	Plaintext in RAM	Power cycle; Switch Approved Mode	SSH Key Exchange Private Key (per SSH 2.0)
SSH_KEX_PUB	ECDH P-256 Curve (128-bits) or FFC DH Group 14 (112-bits)	Generated internally via ECDH or FFC DH	Output encrypted via SSH_SK	Plaintext in RAM	Power cycle; Switch Approved Mode	SSH Key Exchange Public Key (per SSH 2.0)
DRBG Seed	Random bit value	Generated internally	Output encrypted via DEKey	Plaintext in RAM	"Reset" service; Power cycle; Switch Approved Mode	Generate random values for the CTR_DRBG

© Copyright 2017 Oracle Corporation

This document may be freely reproduced and distributed whole and intact including this Copyright notice.

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
DRBG ‘V’ Value	Internal DRBG state value (integer)	Generated internally	Output encrypted via DEKey	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	Output encrypted via DEKey	Plaintext in RAM	“Reset” service; Power cycle; Switch Approved Mode	Internal state value for the CTR_DRBG

© Copyright 2017 Oracle Corporation

This document may be freely reproduced and distributed whole and intact including this Copyright notice.

2.8 EMI/EMC

The StorageTek T10000D 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 T10000D 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, asymmetric key pairs are 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. All test run without requiring operator intervention.

2.9.1 Integrity Tests

An integrity test is the first operation performed by the StorageTek T10000D Tape Drive after power has been supplied. The module performs a 32-bit CRC[53] on the firmware and hardware/FPGA images 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[54]. 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 Approve modes or in the Mixed 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. Otherwise, the module indicates that all self-tests have passed by moving to a normal operational state.

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

[53] CRC – Cyclic Redundancy Check

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

© Copyright 2017 Oracle Corporation

This document may be freely reproduced and distributed whole and intact including this Copyright notice.

- AES ECB Encrypt KAT (OKM agent and firmware)
- AES ECB Decrypt KAT (OKM agent and firmware)
- AES CBC Encrypt KAT (firmware and TLS implementation)
- AES CBC Decrypt KAT (firmware and TLS implementation)
- AES CCM Encrypt KAT (firmware)
- AES CCM Decrypt KAT (firmware)
- AES CCM Encrypt KAT (hardware)
- AES CCM Decrypt KAT (hardware)
- AES Key Wrap KAT (OKM agent)
- RSA Sign/Verify KAT (firmware)
- ECDSA Sign/Verify (firmware)
- SHA-1 KAT (firmware and TLS implementation)
- HMAC SHA-1 KAT (firmware, OKM agent and TLS implementation)
- SHA-256 KAT (firmware)
- SP 800-90A CTR DRBG KAT (firmware)
- ECDH KAT (firmware)
- TLS KDF KAT (TLS implementation)

2.9.3 Conditional Self-Tests

The StorageTek T10000D 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. If the dump file is to be encrypted, the module will 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.

The StorageTek T10000D Tape Drive performs a Pairwise Consistency Test on each Asymetric key pair (RSA and Elliptic Curve) generated in support of establishing a SSH session.

In each mode, 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, the Tape Head interface, or via the Ethernet Interface. The ETD uses a 2048-bit RSA digital signature verification to confirm the integrity of the firmware prior to

© Copyright 2017 Oracle Corporation

This document may be freely reproduced and distributed whole and intact including this Copyright notice.

being loaded onto the module. This test is applied to all loaded firmware including the FPGA firmware components. If the test passes, the module will store the new firmware image in EEPROM. A reboot of the module is required to switch to the new firmware. If the test fails, the new firmware image will be discarded and the module will resume normal operation.

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 T10000D Tape Drive performs the following critical function self-tests:

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

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.

© Copyright 2017 Oracle Corporation

This document may be freely reproduced and distributed whole and intact including this Copyright notice.

3 SECURE OPERATION

The Oracle StorageTek T10000D 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 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#: E20714-08; June 2014)
- *Oracle Virtual Operator Pane 2.2: User's Guide* (Part #: E55615-01; August 2014)
- *Oracle Key Manager: Administration Guide* (Part #: E41579-05; September 2015)

Prior to setting up the StorageTek T10000D 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 T10000D Tape Drive into each of the 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 Approved modes, the CO shall perform the following steps:

1. Install the StorageTek T10000D Tape Drive following the instruction provided in *StorageTek T10000 Tape Drive Installation Manual*
2. Examine the hardware part number on the rear label. Confirm it matches the hardware version number on this Security Policy (Hardware Part #: 7042136/7314405)
3. Verify the VOP version is version 2.2 or higher.
4. 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: RB411111)
5. Using VOP, the CO shall check the Version Tab (Retrieve →View Drive Data) to confirm the version of the FPGAs
    a. CO Hardware Revision: 0000xxxxxxD7

© Copyright 2017 Oracle Corporation

This document may be freely reproduced and distributed whole and intact including this Copyright notice.

b. RO Hardware Revision: xxxx9500
c. DC Hardware Revision: xx050383
d. PRML Hardware Revision: 00004502

6. Enable SSH and SFTP services and disable Peek and Poke services
   a. Set the drive to an "offline" state (Drive Operations → Set Offline)
   b. Using VOP, navigate to the "Network" tab in the "Drive Data" window (Configure → Drive Data)
   c. Set "Telnet Enabled" and "FTP Enabled" to "No"
   d. Set "SSH & SFTP Enabled" to "Yes"
   e. Set "SSH FIPS Mode" to "Yes"
   f. Press the "Commit" button

After pressing the "Commit" button, the ETD will reboot to normal operation.

3.1.2 Encryption Disabled Approved Mode Set-Up

The StorageTek T10000D 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. Set the drive to an "offline" state (Drive Operations → Set Offline)
3. Using VOP, navigate to the "Encrypt" tab in the "View Drive Data" window (Retrieve → View Drive Data)
4. Verify that the "Use OKM or DPKM" Field is set to "UNKN" and the "Permanently encrypting" Field is set to "UNKN". If these fields are not set to these values then follow the steps in 3.2.3 to place the module in the Encryption Disabled Approved Mode.

3.1.3 Encryption Enabled Approved Mode Set-Up

To place the StorageTek T10000D 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. Set the drive to an "offline" state (Drive Operations → Set Offline)
4. Using VOP, navigate to the "Encrypt" tab in the "Drive Data" window (Configure → Drive Data)
5. Set the "Use OKM or DPKM" Field to "OKM"
6. Set the "Permanently encrypting" field to "No"

© Copyright 2017 Oracle Corporation

This document may be freely reproduced and distributed whole and intact including this Copyright notice.

7. Enter a valid Agent ID, Pass Phrase, and OKM IP Address
8. 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 T10000D 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
3. Set the drive to an "offline" state (Drive Operations → Set Offline)
4. Using VOP, navigate to the "Encrypt" tab in the "Drive Data" window (Configure → Drive Data)
5. Set the "Use OKM or DPKM" Field to "OKM"
6. Set the "Permanently encrypting" field to "Yes"
7. Enter a valid Agent ID, Pass Phrase, and OKM IP Address
8. 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 Mixed modes.

3.1.5 Mixed Mode Set-Up

The CO can place the StorageTek T10000D Tape Drive into the Mixed 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. Set the drive to an "offline" state (Drive Operations → Set Offline)
3. Using VOP, navigate to the "Encrypt" tab in the "Drive Data" window (Configure → Drive Data)
4. Set the "Use OKM or DPKM" field to "DPKM"
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 Mixed Mode.

© Copyright 2017 Oracle Corporation

This document may be freely reproduced and distributed whole and intact including this Copyright notice.

3.2 Cryptographic Officer Guidance (Normal Operation)

This section assumes the StorageTek T10000D Tape Drive has been placed into one of the FIPS-Approved modes or the Mixed 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 Approved modes of operation. An Oracle Service Representative is not required to be present when switching Approved modes. Switching between modes will cause keys to be zeroized.

3.2.1 Using SSH (all modes)

The module supports SSH communications for remote administration. SSH is available in each mode of operation. When using SSH for remote administration, only the following options may be used from an SSH client to establish a FIPS-approved session:

1. Protocol Version: SSH v2.0
2. Encryption: AES 128-bit CTR or AES 128-bit CBC
3. MAC: HMAC-SHA-1
4. KEX: ecdh-sha2-nistp256 or diffie-hellman-group14-sha1
5. Host Key: ecdsa-sha2-nistp256, ssh-rsa

Using the preceding options will allow a FIPS-approved SSH session to be established.

3.2.2 Memory Dump Offload (all modes)

Memory dumps may only be offloaded using SFTP (SSH). All other forms of offload are prohibited.

3.2.3 Switching To Encryption Disabled Approved Mode

The CO can place the module into the Encryption Disabled Mode from the Encryption Enabled Mode or the Mixed 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[55]
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

[55] Step 1 is not required if the drive is currently operating in the Mixed Mode

© Copyright 2017 Oracle Corporation

This document may be freely reproduced and distributed whole and intact including this Copyright notice.

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.

3.2.4 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 OKM or DPKM" field to "OKM"
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

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.

3.2.5 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[56]
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 OKM or DPKM" field to "OKM"
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 .

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

© Copyright 2017 Oracle Corporation

This document may be freely reproduced and distributed whole and intact including this Copyright notice.

3.2.6 Switching To Mixed Mode

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

1. Use the "Drive Operations" menu to place the drive offline
2. Navigate to the "Encrypt" tab in the "Drive Data" window (Configure → Drive Data)
3. Set the "Use OKM or DPKM" field to "DPKM"
4. Set the "Permanently encrypting" field to "UNKN"
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 Mixed Mode of Operation.

While in Mixed mode, the CO has available several FIPS-Approved services, including,

1. Firmware Load
2. Remote Management via SSH

Selecting Data Path Key Management (DPKM) to initialize Mixed Mode establishes keys that are established via non-FIPS Approved methods. This provides no cryptographic security for the data that is transformed with the keys. All tape data is considered plaintext in Mixed Mode of operation.

3.3 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 CO shall perform the following steps to zeroize the ETD:

1. Using the "Drive Operations" menu on VOP, reset the ETD (this step is not required if the drive is operating in the Mixed Mode or the Encryption Disabled Approved Mode). The drive will reboot.
2. Using an SSH Client program such as PuTTY or OpenSSH, connect to the ETD using the "cust" account and issue the command "ecpt sshreset". The drive will reboot.
3. Using the "Retrieve" menu in VOP, select "Delete Dumps".

© Copyright 2017 Oracle Corporation

This document may be freely reproduced and distributed whole and intact including this Copyright notice.

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
CRNGT	Continuous Random Number Generator Test
CSE	Communications Security Establishment
CSP	Critical Security Parameter
CRC	Cyclic Redundancy Check
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
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

© Copyright 2017 Oracle Corporation

This document may be freely reproduced and distributed whole and intact including this Copyright notice.

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

© Copyright 2017 Oracle Corporation

This document may be freely reproduced and distributed whole and intact including this Copyright notice.