Sun StorageTek™ T10000B Tape Drive Security Policy

Part Number 316055101
Revision: AB

Sun Microsystems, Inc.

September 1, 2009

TABLE OF CONTENTS

TABLE OF TABLES

Release History

Date	Rev	Description	Name
02/23/09	AA	Initial version of Security Policy as submitted to NIST CMVP, with minor formatting changes. Engineering Change: EC000860	Matt Ball
06/24/09	AB	Updated allowed firmware revisions to include 1.41.210 and 1.41.211, based on change letter to NIST. Included changes based on NIST comments. Engineering Change: EC001172	Matt Ball

1 Module Overview

The Sun StorageTek T10000B Tape Drive (ETD) (HW P/N:315488302; Firmware Versions: 1.40.208, 1.41.210, or 1.41.211) 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 2 security to data on magnetic tape, when operated in FIPS mode.

The ETD can be used in one of two system configurations: Key Management System (KMS) 1.x or KMS 2.x. In the KMS 1.x configuration, the Sun StorageTek Crypto Key Management Station and the Sun StorageTek Key Token (FIPS 140-2 Certificate #993) manage the encryption keys used by the ETD. A Sun StorageTek Key Token acts as a key loader in the context of FIPS 140-2, and can be configured as either an "enabling key token" (EKT) or an "operational key token" (OKT) (see [KMS1UG]). Figure 1 shows the KMS 1.x configuration.

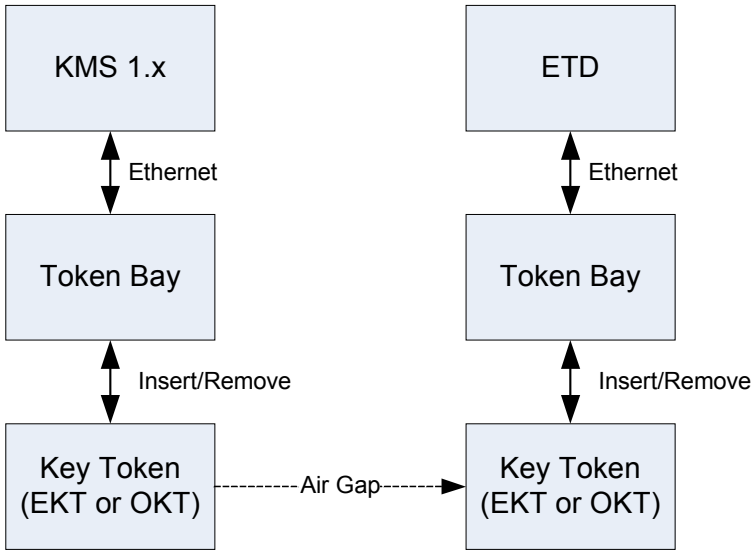

Figure 1: KMS 1.x Component Diagram

In the KMS 2.x configuration, the ETD requests keys from the Sun StorageTek Crypto Key Management System (version 2.1 and higher), which is a cluster of two or more key management appliances. Figure 2 shows the KMS 2.x configuration.

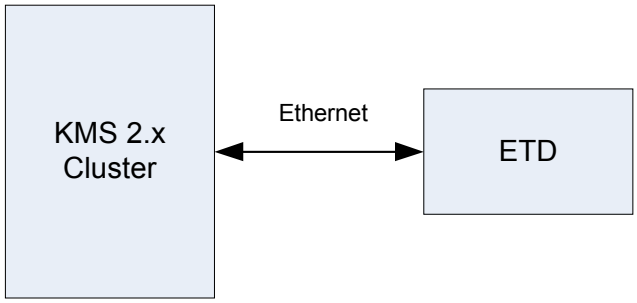

Figure 2: KMS 2.x Component Diagram

For more information on these system components please see the website http://docs.sun.com and browse under Hardware->Tape Storage->Tape Drives.

The cryptographic boundary of the ETD is the external surface of the tape drive's commercial grade metallic enclosure. Excluded from the boundary are the components visible through the tape cartridge slot and the components visible from the ventilation holes. Figure 3 and Figure 4 illustrate the cryptographic boundary as defined:

Figure 3: Front Image of the ETD

Figure 4: Rear Image of the ETD

Note: The picture in Figure 4 is upside-down to show the bottom cover of the ETD.

2 Security Level

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

Table 1: Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	2
Module Ports and Interfaces	2
Roles, Services and Authentication	2
Finite State Model	2

Security Requirements Section	Level
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A

3 Modes of Operation (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: :

- AES CCM supporting 256 bit keys, which provide for the following operations in both hardware (AES Certificate # 495) and firmware (AES Certificate # 647):
    - Encryption
    - Decryption
    - Authentication
- RSASSA-PKCS1-v1_5 supporting 2048 bit keys (RSA Certificate # 334) for digital signature verification (firmware load test)
- HMAC SHA-1 (HMAC Certificate # 398) to create the challenge response as part of the certificate service of the KMS 2.x Agent Toolkit.
- SHA-1 (SHS Certificate # 736) for the following:
    - as part of digital signature verification for the firmware
    - as part of HMAC-SHA-1 (HMAC certificate # 398)
    - for hashing passwords used for authentication
- AES ECB (AES Certificate # 941) 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 # 6) for generating random numbers used for nonce values and cryptographic keys
- AES CTR (AES Certificate # 942) as part of the SP 800-90 CTR DRBG.
- AES CBC mode with 256-bit key (AES Certificate # 967), used within TLS session between ETD and KMS 2.x.
- HMAC-SHA-1 (HMAC Certificate # 540)with 160-bit key used to protect the integrity of TLS communications between the ETD and KMS 2.x.
- SHA-1 (SHS Certificate #937)

- as part of the TLS Key Derivation Functionality
- as part of HMAC SHA-1 (HMAC Certificate # 540)

3.2 Non-Approved Algorithms

The cryptographic module supports the following Non-Approved algorithms that are allowed for use within FIPS Approved mode: MD5 as used within the TLS1.0 Key Derivation Function. (see [TLS1.0])

- AES Key Wrap (AES Certificate #941) 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 is used within the TLS protocol as part of key derivation

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]).

Figure 5 shows the "View Current Drive Settings" of the VOP application (Drive Operations → View Drive Data). The user can tell if the ETD has selected 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.

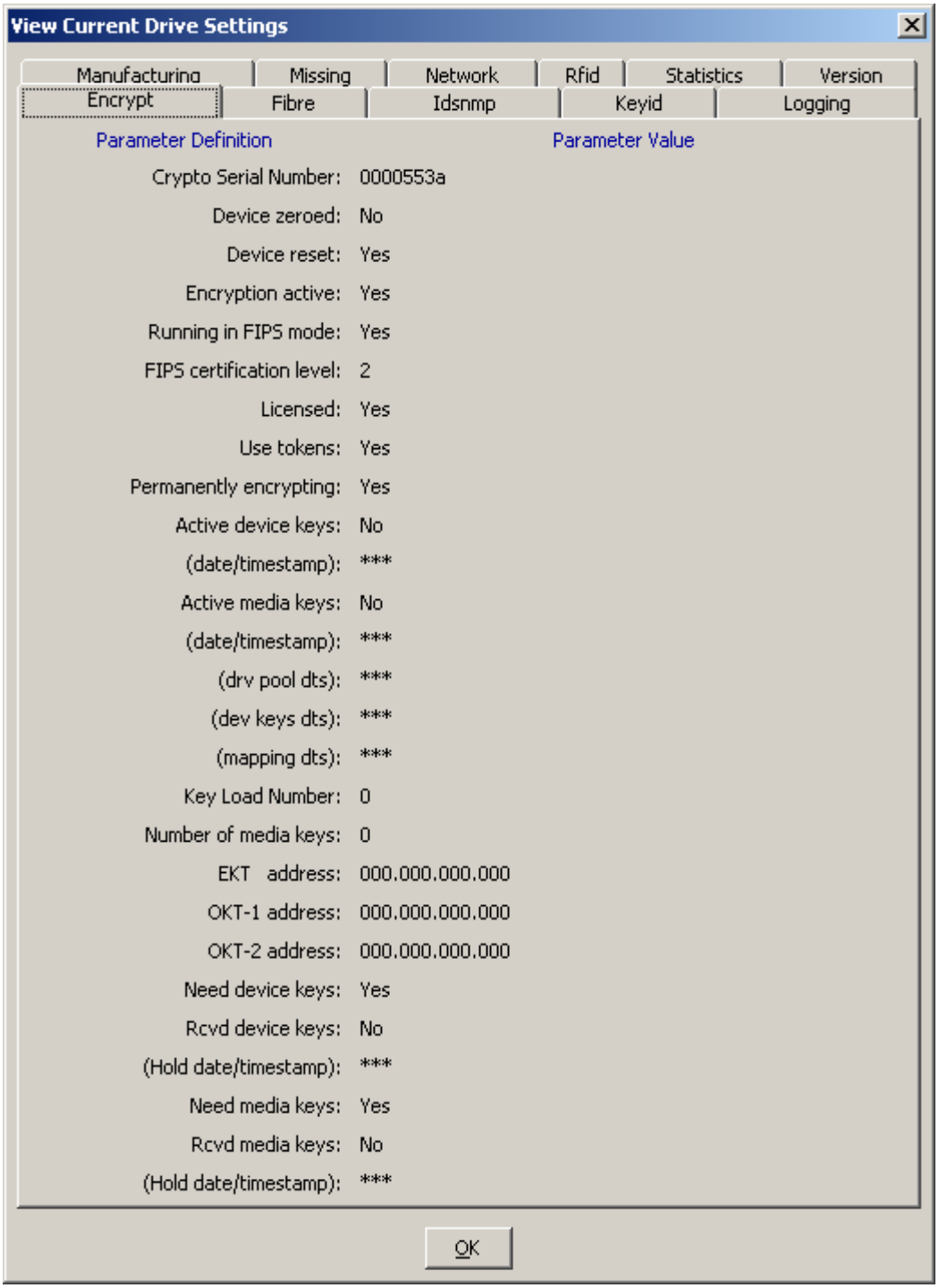

Figure 5: VOP: View Current Drive Settings

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, depending on the configuration.

There are two ways to configure the ETD to be in permanent FIPS 140-2 mode:

1. Insert a valid EKT (Enabling Key Token) into a token bay that is connected to an unlicensed ETD. (see 3.4.1). This is for KMS 1.x only.
2. Use the Virtual Operator Panel (VOP) to license the ETD for encryption and set permanent FIPS mode (see 3.4.2). This is valid for KMS 2.x.

3.4.1 Using an EKT to enable FIPS mode for KMS 1.x

The process of inserting an EKT into an ETD that is not licensed for encryption will, by default, configure the ETD to always encrypt and to enter permanent FIPS mode. For process details on creating an EKT and using it to configure the ETD, see [KMS1UG] ("Enable Encryption in a Drive", Chapter 2).

KMS 1.x FIPS Enable and License Procedure:

1. Create EKT and insert into the Token Bay connected to an unlicensed ETD and wait for the LED to indicate that the ETD has device keys.
2. Issue an IPL and then verify the FIPS status through VOP when the ETD completes a reboot.

3.4.2 Using VOP to enable FIPS mode for KMS 2.x

VOP FIPS 140-2 configuration of ETD requires the presence of both a Sun service representative and the customer. In addition they will need to follow the licensing process as outlined in [KMS2IM] (KMS 2.x Installation and Service Manual), under "License and Enroll the Tape Drives" in Chapter 3 "T-Series Tape Drives".

Both the Sun 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. The service representative shall examine each of the seven tamper evident labels applied to the exterior chassis of the drive to ensure they have not been removed or altered (See section 7 of this document for examination details).
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 bring up the "Configure Drive Parameters" Window (see Figure 7) 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 "Use tokens" field to "No".
   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]).
7. Click on the "Commit" button. The ETD will then reboot and come up in permanent FIPS mode.
8. Verify that FIPS mode was correctly set by examining the FIPS status (see 3.3).

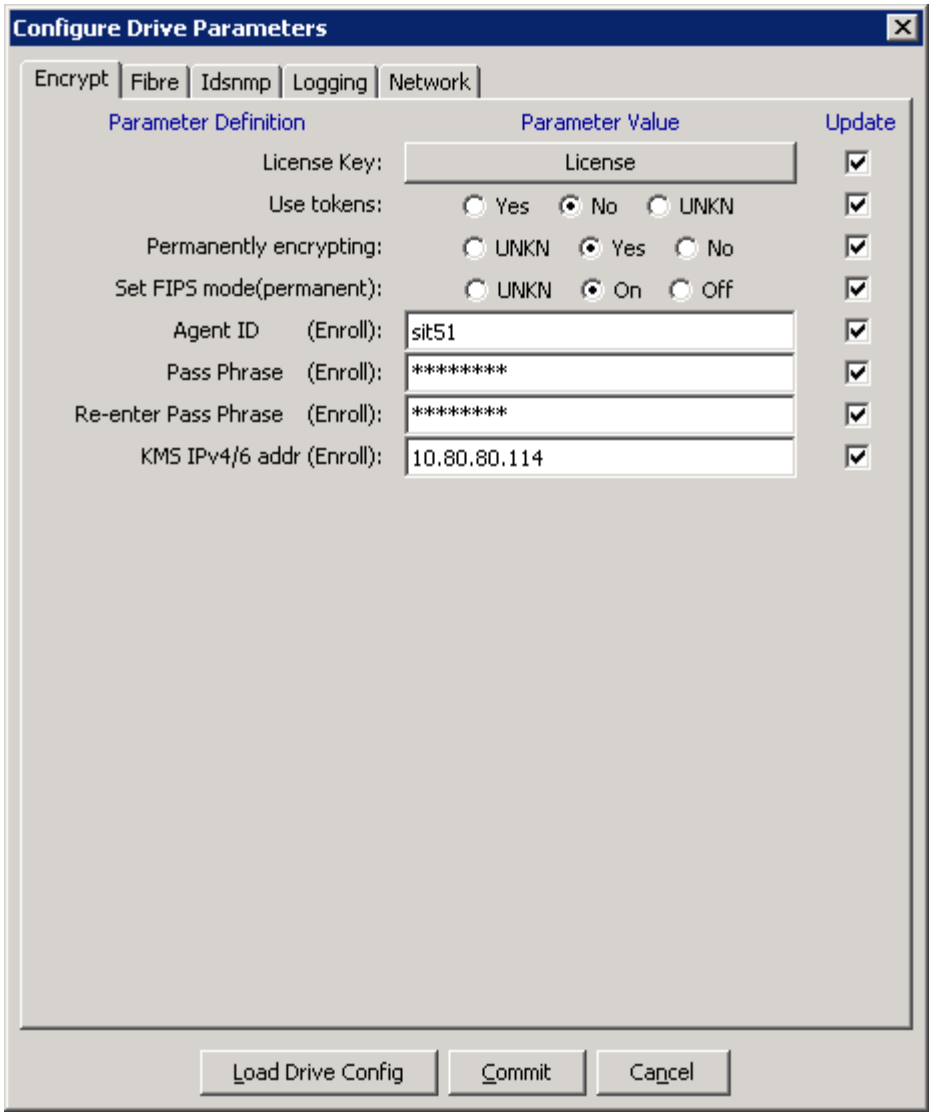

Figure 7: VOP: "Configure Drive Parameters" Window

4 Ports and Interfaces

This section describes all ports and interfaces supported by the Tape Drive. Table 2 below provides a listing of the following 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	Primarily used for tape library communications.

Physical Port	Qty	Logical interface definition	Technical Specification
Host Interface	2	data input, data output, status output, control input	This interface is used to transfer user data between the ETD and the host. When the host transfers user data to the ETD through this interface, the ETD encrypts and writes the data to the magnetic media. When the host receives user data from the ETD through this interface, the ETD delivers data read from the magnetic media that has been decrypted by the ETD. The interface can be configured to support one of two protocols: 1) Fibre Channel, in accordance with the Fibre Channel Protocol-3 (FCP-3)[1], SCSI Primary Commands-3 (SPC-3), and SCSI Stream Commands (SSC-3) specifications [8] 2) FICON, in accordance with the Fibre Channel Single-Byte Command Code Sets-3 Mapping Protocol (FC-SB-3), Revision 1.6 specification [9]
Tape head	1	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).
Operator Panel Connector	1	status output, control input	A 20-pin connector (located on the bottom of the ETD) that is designed to connect to a Rack Mount Operator Panel. This connector includes wires that are designed to hook to the following external components: 1) Four LED's to provide status output. 2) An LCD display is used to display ETD status and configuration menu text. 3) Four push button micro-switches. Two of the four switches are used to navigate through the ETD configuration menus. The other two switches are used to rewind/unload a cartridge, reboot the ETD, and to enter Boot Monitor mode at power-up. NOTE: The three interfaces listed directly above are not part of the Tape Drive. They reside on an optional Sun Microsystems External Rack Mount Chassis into which two Tape Drives may be inserted.
Power Interface	1	power input	88-264 VAC @ 48-63 Hz
Drive Status LED	1	status output	Provides status on the overall state of the ETD

Physical Port	Qty	Logical interface definition	Technical Specification
Encryption Status LED	1	status output	Provides status on the encryption configuration of the ETD.
Rear Panel Switch	1	control input	Used by the service representative to temporarily set the ETD's IP settings to factory default values.
RFID Reader	1	data input, data output	Allows the tape drive to obtain control input from the RFID chip inside the magnetic tape cartridge. The RFID chip contains information that includes: 1) The state of the Media Information Record(MIR) 2) Location of the MIR and End-Of-Data (EOD) on tape 3) Cartridge type 4) The write operations count 5) Manufacturing information (e.g. serial number) 6) Certain performance/usage statistics
RJ45(Ethernet)	1	data input, data output, status output, control input	This primary uses of this interface are 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 server.

5 Identification and Authentication Policy

5.1 Assumption of roles

The ETD cryptographic module shall support two distinct authenticated operator roles, User and Crypto-Officer (C.O.). Table 3 shows the roles and authentication methods.

Table 3: Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
User	Role-based operator authentication.	Any of the following Authentication Mechanisms (see Table 4) are allowed for authenticating the User Role: 1. OC_Key:256-bit AES key 2. CA_Cert Private Key: 2048-bit RSA Private key
Crypto-Officer	Role-based operator authentication.	Any of the following Authentication Mechanisms (see Table 4) are allowed for authenticating the Crypto-Officer Role: 1. VOP Password: 7 byte shared secret. 2. Passphrase: 8 byte shared secret. 3. PC_Key: 256-bit AES key 4. DS_Key: 256-bit AES key 5. FSRootCert: 2048-bit private RSA key

Table 4 shows the strengths of authentication mechanisms for assuming each supported role based on the following descriptions of table headings:

- **Authentication Mechanism**: This is the CSP (critical security parameter) or public key used to authenticate an operator.
- **Strength of Mechanism Per Guess:** This is the probability that a single random authentication attempt succeeds. To meet FIPS 140-2 requirements, this probability needs to be less than 1 in 1,000,000.
- **Strength of Mechanism Per Minute**: This is the probability that a series of random authentications succeeds over a one minute period. To meet FIPS 140-2 requirements, this probability needs to be less than 1 in 100,000.

Table 4: Strengths of Authentication Mechanisms

Authentication Mechanism	Description	Strength of Mechanism Per Guess	Strength of Mechanism Per Minute
VOP Password	A 7 character password chosen from the set of 96 printable ASCII characters used to authenticate a Crypto-Officer. Each guess is throttled by the data rate of the Ethernet port, at 100 MBits/s.	The probability that a random attempt succeeds or a false acceptance occurs is no greater than 1 in 75,144,747,810,816 (96^-7), which is less than 1 in 1,000,000.	The ETD allows fewer than 4,687,500 (at 100 MBits/s, assuming a send and receive packet of 64 bytes each for each attempt, and 10 bits per byte encoding) authentication attempts in a one minute period; therefore the random success rate for multiple retries is 1 in 16030879 (=4,687,500 /96^7).
Passphrase	A minimum 8 character password, selected from the set of 96 printable ASCII characters used to authenticate a Crypto-Officer. The Passphrase is stretched using SHA-1 such that it takes 1/10 of a second to compute the Authentication Secret.	1 in 7.2×10^{15} (=1 in 96^8).	1 in 1.2×10^{13} (based on 600 attempts per minute).
FSRootCert	A 2048-bit RSA signing key (with 112 bits of strength) used for signing firmware image. Verified using FSRootCert.	Chance of guessing private key is 1 in 2^{112} per attempt.	No more than one attempt is allowed each millisecond, which means that no more than 60,000 attempts are allowed in a one minute period, putting the chance of guessing the RSA private key to 1 in (2^{112})/60,000.

Authentication Mechanism	Description	Strength of Mechanism Per Guess	Strength of Mechanism Per Minute
PCKey (Via Token)	A 256-bit AES CCM key used to authenticate a Crypto-Officer during the licensing phase and enrollment phase	Chance of guessing PCKey and authenticating is 1 in 10^{77} (2^{256}).	In a one minute period, the chance of a successful authentication is less than 1 in 10^71. (This is limited by traffic over a 100Mbps Ethernet link, with minimum packet size of 70 bytes and an assumed 10 bits per byte encoding)
DSKey (Via Token)	A 256-bit AES CCM key used to authenticate a Crypto-Officer. NOTE: This key is only a CSP in the 1.x configuration. In the 2.x configuration this key. In a 2.x configuration this key will not exist.	Chance of guessing DSKey and authenticating is 1 in 10^{77} (2^{256}).	In a one minute period, the chance of a successful authentication is less than 1 in 10^71. (See rationale for PCKey)
OCKey (Via Token)	A 256-bit AES CCM key used to authenticate a User NOTE: This key is only categorized as a CSP in the 1.x configuration. In the 2.x configuration this key will not exist.	Chance of guessing OCKey and authenticating is 1 in 10^{77} (2^{256}),	In a one minute period, the chance of a successful authentication is less than 1 in 10^71. (See rationale for PCKey)
CA_Cert Private Key	A 2048-bit RSA private key (with 112-bits of strength) that corresponds to the public key within the CA_Cert Used to authenticate the server during the TLS handshake.	Chance of guessing private key is 1 in 5.2 x 10^{33} (2^{112}) per attempt.	No more than one attempt is allowed each millisecond, which means that no more than 60,000 attempts are allowed in a one minute period, putting the chance of guessing the RSA private key to 1 in (2^112)/60,000.

6 Definition of Critical Security Parameters (CSPs)

Table 5 describes the CSPs that are contained within the ETD.

Table 5: Description of Critical Security Parameters (CSPs)

CSP	Description/Usage
Preset Communication Key (PCKey)	The Preset Communication Key is a 256-bit AES key loaded into the ETD during manufacturing. In the KMS 2.x configuration, the PCKey is used for encryption licensing. In the KMS 1.x configuration, the PCKey is used to enable encryption

CSP	Description/Usage
	within a new ETD, and to reinitialize an ETD after the Reset service has been used.
Communication Key (OCKey)	A Communication Key is a 256-bit AES key used in the KMS 1.x configuration to encrypt communications between an OKT and an ETD. The OCKey is also used to provide mutual-authentication between an OKT and an ETD.
Device Split Key (DSKey)	A Device Split Key is a 256-bit AES key used in the KMS 1.x configuration to protect Media Keys and to support device key updates from an EKT after an ETD has been initialized.
Media Key (MEKey)	Media Keys are 256-bit AES CCM keys which are generated outside the Tape Drive by either the KMS 1.x or the KMS 2.x. An ETD uses a MEKey to encrypt and decrypt the customer bulk data it processes.
Wrap Key (WKey)	A Wrap Key is a 256-bit AES keys used in the KMS 1.x configuration to wrap a set of DSKey (MEKey xor DSKey), KeyID pairs. The objective of this process is to add an additional layer of encryption security beyond that provided by DSKey.
Passphrase	This is an 8-byte character string supplied independently to both the ETD and the KMS 2.x cluster as part of the enrollment process in the KMS 2.x configuration. The Passphrase must contain characters from at least three of the four character classes, and has a minimum length configurable by the end user. The Passphrase is used to mutually authenticate the ETD and KMS 2.x during first time authentication, and is erased from drive memory when the enrollment process completes.
VOP Password (TelnetPW)	A 7-byte shared secret used to authenticate an operator the Crypto-Officer Role.
CTR_DRBG	The CSPs within the SP 800-90 CTR DRBG are an AES-256 key , the 128-bit value *V*, and a reseed counter. The CTR_DRBG generates random numbers 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 ME_Keys with AES Key Wrap as they enter the ETD
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.
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 a appliance within a KMS 2.x cluster.
CA_Private Key	The CA_Cert Private Key is for authentication of the appliance during TLS1.0 communication between the ETD and a KMS 2.x cluster.
FSRootCert Private Key	The FSRootCert Private Key is used to authenticate the firmware updates by authenticating the final firmware signing key in a certificate chain.
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	Enccrypt 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)

CSP	Description/Usage
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 6 describes the public keys stored with the ETD.

Table 6: 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 (KWKPublicKey)	The Key Wrap Key Public Key is a 2048-bit RSA public key used to wrap the 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 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 7 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 7: Services Authorized for Roles

Name of Service	Service Description	Available on:	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)	C.O.	Uses Passphrase; Writes and uses CA_Cert; Writes TDPrivKey; Writes TDPubKey

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 8. None of the services modify, disclose, or substitute cryptographic keys and CSPs, or otherwise affect the security of the ETD.

Table 8: Unauthenticated Services

Name of Service	Service Description	Available On:
Show Status	Provides the current status of the ETD.	Drive Status LED, Encryption Status LED, Operator Panel Connector, RJ45(Ethernet), Host Interface, DB15(RS232)
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 9.1 .	Power Interface
Fibre Channel Interface Management	Provides non-security relevant ETD management and status output (see [ETDIR]).	Host Interface
LibraryManagement	Provides non-security relevant ETD management and status outputof the ETD.	DB15 (RS232)
Operator Panel	Provides non-security relevant ETD management and status output. See [ETDOG] for details.	Operator Panel Connector
Rear Panel Switch	Mechanical switch located on the rear of the ETD that allows the module to enter the boot monitor mode.	Rear Panel Switch

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 (verification only)
      ii) Firmware Integrity Test (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, 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.

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 opaque enclosure
- Tamper evident labels

The following figures (Figure 8, Figure 9, and Figure 10) show the locations of the seven tamper-evident seals on the ETD. The seals are identified by a red circle.

Figure 8: Tamper Evident Seals on Left Side

Figure 9: Tamper Evident Seals on Right Side

Figure 10: Tamper Evident Seal on Bottom

Upon secure receipt of the ETD cryptographic module, the operator shall examine all seven tamper-evident seals to determine whether the ETD has been compromised. If any of the seven tamper-evident labels show evidence of tampering, then the module is not physically secure and is no longer compliant with FIPS 140-2.

The following list describes possible ways that the tamper-evident labels show evidence of tampering:

1. The pattern “Void” is visible through the tamper-evident label.
2. One or more corners of the tamper-evident label is lifted.
3. The tamper-evident label is missing.
4. A tamper-evident label on the sides is misplaced such that it does not touch two metal covers.
5. The tamper-evident label on the bottom is misplaced such that it does not cover the screw that secures the front bezel (honeycomb grate that allows airflow).

10.2 Required Operator Actions

The operator is required to periodically inspect tamper evident seals using the following guidance found in Table 9:

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper-Evident Seals	Per internal security policy requirements of ETD customer.	Inspect seven tamper seals; three on the left side, three on the right

		side, and one on the bottom.

Table 9: Inspection/Testing of Physical Security Mechanisms

11 Mitigation of Other Attacks Policy

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

12 References

[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

[ETDIR] T10000 Tape Drive: Interface Reference Manual, Sun Microsystems, Part Number MT9259J. Available at http://docs.sun.com/app/docs/doc/MT9259J.

[ETDOG] Sun Microsystems T10000 Operator's Guide, Part No. 96174, Rev. EB. Available at http://docs.sun.com/app/docs/doc/96174revEB.

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

[FCP-3] Fibre Channel Protocol-3 (FCP-3), SCSI Primary Commands-3 (SPC-3), and SCSI Stream Commands (SSC-3) specifications

[KMS1UG] Sun Key Management Station Users Guide, Part No. 96262, Rev B. Available at http://docs.sun.com/app/docs/doc/CRCM2146

[KMS2IM] KMS 2.0 Installation and Service Manual (Rev. BA), Part Number 316194903BA, Sun Microsystems. June 2008. Available at http://docs.sun.com/app/docs/doc/316194903BA.

[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".

[VOPUG] Virtual Operator Panel User's Guide (Customer) rev JA, Sun Microsystems, Part Number 96179JA, April 2008. Available at http://docs.sun.com/app/docs/doc/96179revJA.

13 Definitions and Acronyms

AES	Advanced Encryption Standard
CO	Crypto-Officer
ETD	The Sun StorageTek T10000B Tape Drive.
IPL	Initial Program Load. The process that brings up the ETD after a power-on or reset.
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