IBM System Storage TS1140 Tape Drive – Machine Type 3592, Model E07

Security Policy

Document Version 1 Revision 17

Table of Contents

1 Document History

Date	Author	Change
05/06/2011	Said Ahmad	V0.0 Initial Creation
07/27/2012	Said Ahmad	V1.0 Remove old cert numbers and replace PRNG with DRBG
08/06/2012	Said Ahmad	V1.1 Remove references to 1024-bit RSA key
9/27/2012	Said Ahmad	V1.2 Replace RNG with DRBG
02/05/2013	Christine Knibloe	V1.3 Update DRBG information. Add SHA-512 information.
04/17/2013	Christine Knibloe	V1.4 Updates from onsite test results. Update algorithm certificates.
04/22/2013	Christine Knibloe	V1.5 DRBG algorithm certificate
04/29/2013	Christine Knibloe	V1.6 Add details for RSA and AES
05/10/2013	Christine Knibloe	V1.7 Incorporate SAIC feedback
05/13/2013	Christine Knibloe	V1.8 Update DRBG information
05/31/2013	Christine Knibloe	V1.9 Incorporate additional feedback
05/31/2013	Christine Knibloe	V1.10 Incorporate additional feedback
02/04/2014	Said Ahmad	V1.11 Incorporate additional feedback
03/06/2014	Said Ahmad	V1.12 Incorporate additional feedback
04/02/2014	Said Ahmad	V1.13 Incorporate additional feedback
05/27/2014	Said Ahmad	V1.14 Add key wrapping to AES usage
06/16/2014	Said Ahmad	V1.15 Restate the secure configuration statement
06/19/2014	Said Ahmad	V1.16 Add HMAC entry to table 6
06/19/2014	Said Ahmad	V1.17 Remove references to unused HMAC

2 Introduction

The security policy document is organized in the following sections:

- Introduction
- References
- Document Organization

This non-proprietary security policy describes the IBM System Storage TS1140 Encrypting Tape Drive - Machine Type 3592, Model E07 cryptographic module and the approved mode of operation for FIPS 140-2, security level 1 requirements. This policy was prepared as part of FIPS 140-2 validation of the TS1140. The IBM System Storage TS1140 Tape Drive - Machine Type 3592, Model E07 is referred to in this document as the "TS1140 Encrypting Tape Drive," the "TS1140," and the encrypting Tape Drive.

Table 1: Security Section

Security Section	Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services, and Authentication	1
Finite State Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A
Overall	1

FIPS 140-2 (Federal Information Processing Standards Publication 140-2—*Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the NIST web site at:

http://csrc.nist.gov/groups/STM/cmvp/

TS1140 Encrypting Tape Drive Cryptographic Module Description

- Cryptographic Module Overview
- Secure Configuration
- Cryptographic Module Ports and Interfaces
- Roles and Services
- Physical Security
- Cryptographic Key Management
- Self-Tests
- Design Assurance
- Mitigation of Other Attacks

2.1 References

This document describes only the cryptographic operations and capabilities of the TS1140 Encrypting Tape Drive. More information is available on the general function of the TS1140 Encrypting Tape Drive at the IBM web site:

http://www.ibm.com/storage/tape/

The tape drive meets the T10 SCSI-3 Stream Commands (SSC) standard for the behavior of sequential access devices. In addition, the tape drive primary host interfaces are physical fibre channel ports. The physical and protocol behavior of these ports conforms to Fibre Channel Protocol (FCP) specification. These specifications are available at the INCITS T10 standards web site:

http://www.T10.org /

A Redbook describing tape encryption and user configuration of the TS1140 drive in various environments can be found at:

http://www.redbooks.ibm.com/abstracts/sg247320.html?Open

The TS1140 drive format on the tape media is designed to conform to the IEEE P1619.1 committee draft proposal for recommendations for protecting data at rest on tape media. Details on P1619.1 may be found at:

http://ieeexplore.ieee.org/servlet/opac?punumber=4413113

2.2 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
- Other supporting documentation and additional references

3 TS1140 Encrypting Tape Drive Cryptographic Module Description

3.1 Overview

The TS1140 Encrypting Tape Drive is a set of hardware, firmware, and interfaces allowing the optional storage and retrieval of encrypted data to magnetic tape cartridges. The entire "brick" unit of the TS1140 tape drive is FIPS certified as a multi-chip, standalone cryptographic module. In customer operation the "brick" unit is embedded in a canister package and may be used in conjunction with a computer system or tape library. Some components of the TS1140 tape drive, such as mechanical components used for tape loading/unloading and actuating the tape cartridge, labels, cables, connectors, terminals and sensor components, do not have an effect on the security of the cryptographic module, **and thus are excluded from the module boundary.**

The hardware and firmware versions are controlled as specified in section 3.7, with the FIPS certified Hardware EC Level being 00V6759 EC Level M11776 and the Firmware EC Level being 35P2401 EC Level M11776.

A block diagram of the TS1140 Encrypting Tape Drive is shown below:

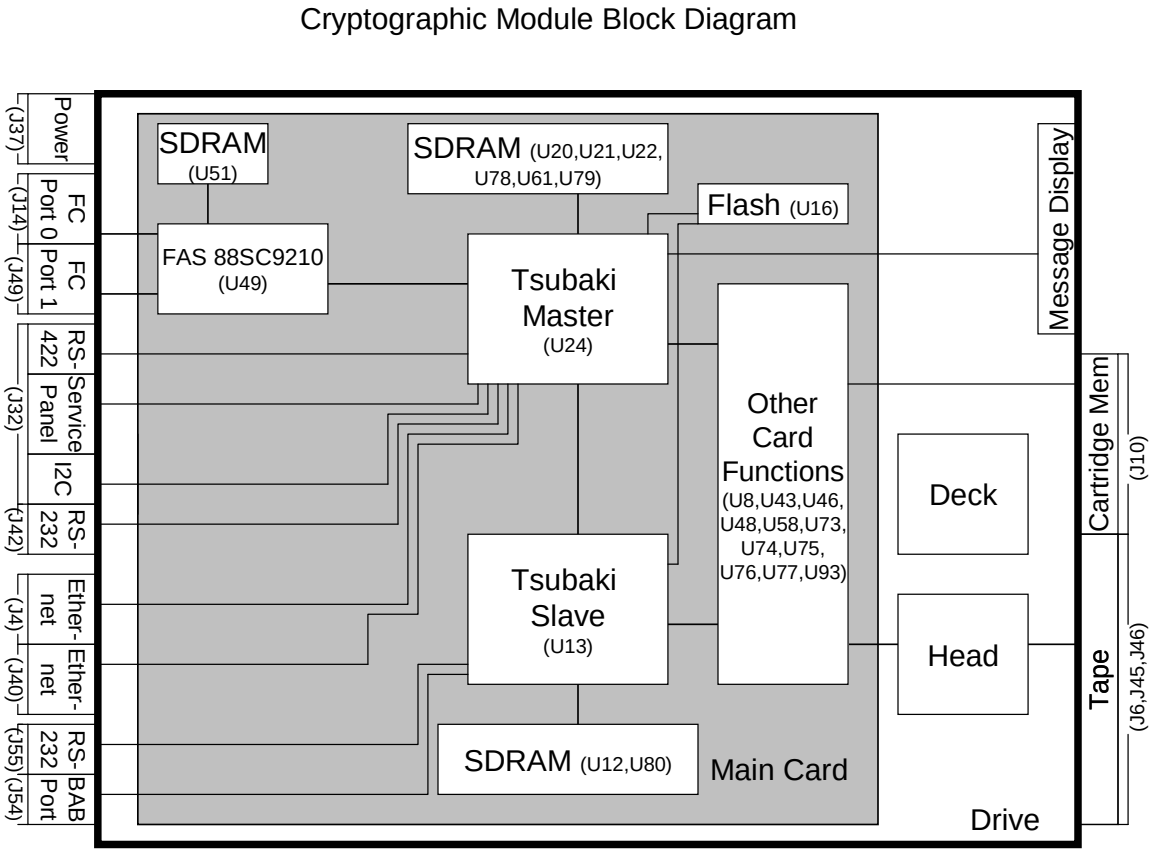


Figure 1: TS1140 Block Diagram

The TS1140 Encrypting Tape Drive has two major cryptographic functions:

- Data Block Cipher Facility: The tape drive provides functions which provide the ability for standard tape data blocks as received during SCSI-type write commands to be encrypted before being recorded to media using AES-GCM block cipher using a provided key, and decrypted during reads from tape using a provided key.
    - Note the AES-GCM block cipher operation is performed after compression of the host data therefore not impacting capacity and data rate performance of the compression function
    - The TS1140 drive automatically performs a complete and separate decryption and decompression check of host data blocks after the compression/encryption process to validate there were no errors in the encoding process
- Secure Key Interface Facility: The tape drive provides functions which allow authentication of the tape drive to an external IBM key manager, such as the IBM Encryption Key Manager (EKM) or the Tivoli Key Lifecycle Manager (TKLM), and allow transfer of protected key material between the key manager and the tape drive.

3.2 Secure Configuration

This section describes the approved mode of operation for the TS1140 drive to maintain the FIPS 140-2 validation.

There is only one FIPS approved mode of operation for the TS1140 which could be configured in two different configurations in the approved mode of operation. They are:

- System-Managed Encryption (SME)
- Library-Managed Encryption (LME)

In order to be in an approved mode of operation, the values of the fields Key Path (manager Type) (from VPD), In-band Key Path (Manager Type) Override, Indirect Key Mode Default, Key Scope, and Encryption Method must be set according to the table below. More details can be found in the TS1140 SCSI Reference.

Table 2: Settings for Approved Configurations

Required Fields	System-Managed Encryption (SME)	Library-Managed Encryption (LME)
Key Path (Manager Type) (from VPD) Mode Page X'25', byte 21, bits 7-5	001b	110b
In-band Key Path (Manager Type) Override Mode Page X'25', byte 21, bits 4-2	000b or 001b	000b
Indirect Key Mode Default Mode Page X'25', byte 22, bit 4	0b	0b
Key Scope Mode Page X'25', byte 23, bits 2-0	000b or 001b	000b or 001b
Encryption Method Mode Page X'25', byte 27	10h or 1Fh	60h

A user can determine if the TS1140 is in the approved mode of operation by issuing a SCSI Mode Sense command to Mode Page X'25' and evaluating the values returned.

Certain commands are prohibited while in the approved mode of operation. The commands vary based on which configuration is used in the approved mode. In the LME configuration, all Mode Select commands to subpages of Mode Page X'25' and Mode Page X'30', Subpage X'20' are prohibited. In the SME configuration, Mode Select commands to the following subpages of Mode Page X'25' and Mode Page X'30', Subpage X'20' are prohibited.

Table 3: Mode Select Eligibility of Mode Page X'25' Subpages

Mode Page	Mode Subpages	System-Managed Encryption (SME)	Library-Managed Encryption (LME)
X'25'	X'C0' – Control/Status	**Allowed**	Prohibited
X'25'	X'D0' – Generate dAK/dAK' Pair	Prohibited	Prohibited
X'25'	X'D1' – Query dAK	Prohibited	Prohibited
X'25'	X'D2' – Update dAK/dAK' Pair	Prohibited	Prohibited
X'25'	X'D3' – Remove dAK/dAK' Pair	Prohibited	Prohibited
X'25'	X'D5' – Drive Challenge/Response	**Allowed**	Prohibited
X'25'	X'D6' – Query Drive Certificate	**Allowed**	Prohibited
X'25'	X'D8' – Install eAK	Prohibited	Prohibited
X'25'	X'D9' – Query eAK	Prohibited	Prohibited
X'25'	X'DA' – Update eAK	Prohibited	Prohibited
X'25'	X'DB' – Remove eAK	Prohibited	Prohibited
X'25'	X'DF' – Query dSK	**Allowed**	Prohibited
X'25'	X'E0' – Setup SEDK/EEDK(s)	**Allowed**	Prohibited
X'25'	X'E1' – Alter EEDK(s)	**Allowed**	Prohibited
X'25'	X'E2' – Query EEDKs (Active)	**Allowed**	Prohibited
X'25'	X'E3' – Query EEDKs (Needed)	**Allowed**	Prohibited
X'25'	X'E4' – Query EEDKs (Entire)	**Allowed**	Prohibited
X'25'	X'E5' – Query EEDKs (Pending)	**Allowed**	Prohibited
X'25'	X'EE' – Request EEDKs (Translate)	**Allowed**	Prohibited
X'25'	X'EF' – Request EEDKs (Generate)	**Allowed**	Prohibited
X'25'	X'FE' – Drive Error Notify	**Allowed**	Prohibited
X'30'	X'20' – Encryption Mode	Prohibited	Prohibited

Loading a FIPS 140-2 validated drive microcode level and configuring the drive for SME or LME operation initializes the TS1140 into the approved mode of operation. To ensure that the FIPS 140-2 validated drive microcode level occupies both the main and reserved firmware locations, it's suggested that the firmware be loaded twice.

The TS1140 supports multi-initiator environments, but only one initiator may access cryptographic functions at any given time. Therefore the TS1140 does not support multiple concurrent operators.

The TS1140 implements a non-modifiable operational environment which consists of a firmware image stored in FLASH. The firmware image is copied to, and executed from, RAM. The firmware image can only be updated via FIPS-approved methods that verify the validity of the image.

The TS1140 drive operates as a stand-alone tape drive and has no direct dependency on any specific operating system or platform for FIPS approved operating mode, but does have requirements for:

- Key Manager/Key Store attachment
- Drive Configuration

The following criteria apply to the usage environment:

- Key Manager and Key Store Attachment
  - In both SME and LME configurations, an IBM key manager, such as the Encryption Key Manager (EKM) or the Tivoli Key Lifecycle Manager (TKLM), and a supported key store must be used in a manner which supports secure import and export of keys with the TS1140 drive :
    - Keys must be securely passed into the TS1140 drive. The key manager must support encryption of the Data Key to form an Session Encrypted Data Key (SEDK) for transfer to the TS1140 drive using the TS1140 drive public Session Key and a 2048-bit RSA encryption method.
    - The key manager/key store must be able to use the EEDK it supplies the drive to determine the Data Key.
- Drive Configuration requirements
  - The TS1140 drive must be configured in SME or LME configurations.
  - The TS1140 drive must have the FIPS 140-2 validated drive firmware level loaded and operational.
  - Drive must be configured in the approved mode of operation.
  - In LME configuration, the TS1140 drive must be operated in an automation device which operates to the LDI or ADI interface specifications provided.

3.3 Ports and Interfaces

The cryptographic boundary of the TS1140 drive cryptographic module is the drive brick. Tape data blocks to be encrypted (write operations) or decrypted data blocks to be returned to the host (read operation) are transferred on the host interface ports using SCSI commands, while protected key material may be received on the host interface ports or the library port.

The physical ports are separated into FIPS-140-2 logical ports as described below.

Table 4: Ports and Interfaces of the TS1140

TS1140 Drive Physical Ports	**FIPS-140-2 Logical Interface**	**Crypto Services**	**Interface Functionality**
Fibre Channel Port 0 Fibre Channel Port 1	Data Input Data Output Control Input Status Output	Yes	▪ Inputs data ▪ Crypto: Inputs protected keys from the key manager in SME configuration. ▪ Outputs data ▪ Outputs encrypted key components ▪ Inputs SSC-3 SCSI protocol commands ▪ Outputs SSC-3 SCSI protocol status
RS-422 Port	Data Input Data Output Control Input Status Output	Yes	▪ Crypto: Inputs protected keys from the key manager in LME configuration. ▪ Outputs data ▪ Outputs encrypted key components ▪ Inputs LDI and LMI protocol commands. ▪ Outputs LDI and LMI protocol status.
RS-232 Ports	Disabled	None	▪ Disabled in the FIPS validated firmware
Ethernet Port	Control Input Status Output Data Input	None	▪ Inputs controls and image for firmware load ▪ Outputs status
BAB Port	Disabled	None	▪ Disabled by FIPS approved firmware levels.
I2C Interface	Data Input Data Output	None	▪ Inputs VPD data ▪ Outputs VPD data
Service Panel Interface	Control Input Status Output	Yes	▪ Inputs controls from service panel ▪ Crypto: Inputs controls for key zeroization ▪ Crypto: Inputs controls for VPD configuration ▪ Outputs status ▪ Crypto: Outputs indicator for the encrypting state
Front Panel Interface - 8 Character Display - Unload Button - Reset Button	Control Input Status Output	Yes	▪ Inputs unload button selection ▪ Inputs reset button selection ▪ Outputs status on 8 character display ▪ Crypto: Outputs indicator for the encrypting state
Input Power Port	Power	None	▪ Inputs power to the TS1140 drive
Cartridge Memory RFID Port	Data Input Data Output	Yes	▪ Inputs parameters. ▪ Crypto: Inputs external key structures ▪ Outputs parameters. ▪ Crypto: Outputs external key structures
Read/Write Head	Data Input Data Output Control Input	None	▪ Inputs data from tape cartridges (decrypted reads) ▪ Outputs data to tape cartridges (encrypted writes) ▪ Inputs command to load firmware from special FMR cartridges

3.4 Roles and Services

The TS1140 drive supports both a Crypto Officer role and a User role, and uses basic cryptographic functions to provide higher level services. For example, the TS1140 drive uses the cryptographic functions as part of its data reading and writing operations in order to perform the encryption/decryption of data stored on a tape.

The Crypto Officer role is implicitly assumed when an operator performs key zeroization. The User role is implicitly assumed for all other services. Both operators have access to the Power-up Self-Tests service.

The two main services the TS1140 drive provides are:

- Encryption or decryption of tape data blocks using the Data Block Cipher Facility.
- Establishment and use of a secure key channel for key material passing by the Secure Key Interface Facility.

It is important to note that the Secure Key Interface Facility may be an automatically invoked service when a user issues Write or Read commands with encryption enabled that require key acquisition by the TS1140 drive. Under these circumstances the TS1140 drive automatically establishes a secure communication channel with a key manager and performs secure key transfer before the underlying write or read command may be processed.

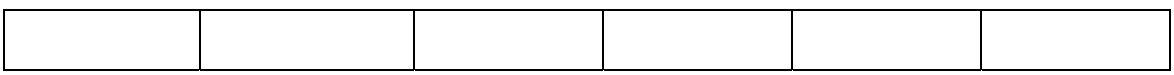
3.4.1 User Guidance

The services table describes what services are available to the User and Crypto Officer roles.

- There is no authentication required for accessing the User Role
- There is no authentication required for accessing the Crypto Officer Role

Single Operator requirements:

- The TS1140 drive enforces a requirement that only one host interface initiator may have access to cryptographic services at any given time.



3.4.2 Provided Services

Available services are also documented in the specified references. All of the services summarized here, excluding the services expressly prohibited in Table 3, are allowed in the FIPS mode of operation.

Table 5: Provided Services

Service	Interface(s)	Description	Inputs	Outputs	Role
General SCSI commands	- Host	As documented in the TS1140 SCSI Reference	Formatted Operational Codes and Messages	Formatted Operational Codes and Messages	User
General Library Interface commands	- Library	As documented in the Drive Library LDI and LMI Interface Specifications	Formatted Operational Codes and Messages	Formatted Operational Codes and Messages	User
Service Panel Configuration	- Service Panel	Set selected aspects of drive configuration manually, per the 3592 E07 Maintenance Information Manual	Button selections	Service Panel	User
Service Panel Diagnostics	- Service Panel	Invoke diagnostics manually, per the 3592 E07 Maintenance Information Manual	Button selections	Service Panel, 8 Character Display	User
Service Panel Status Display	- Service Panel	Displays status, per the 3592 E07 Maintenance Information Manual	From TS1140 drive operating system	Service Panel	User
Front Panel Interface Status	- Front Panel Interface (8 Character Display)	Displays status, per the 3592 E07 Maintenance Information Manual	From TS1140 drive operating system	8 Character Display	User
Front Panel Interface Unload	- Front Panel Interface (Unload Button)	Unload via unload button	Button selection	8 Character Display	User
Front Panel Interface Reset	- Front Panel Interface (Reset Button)	Reset via the reset button	Button selection	Reboot occurs	User

Service	Interface(s)	Description	Inputs	Outputs	Role
Encrypting Write-type Command	- Host	The Secure Key Interface Facility automatically requests a key, provides authentication data, securely transfers and verifies the key material. The Data Block Cipher Facility encrypts the data block with the received Data Key using AES-GCM block cipher for recording to media. A received EEDK is automatically written to media using the Cartridge memory and the RW Head Interface. The decryption-on-the-fly check performs AES-GCM decryption of the encrypted data block and verifies the correctness of the encryption process	- Plaintext data - SEDK - EEDK	- Encrypted data on tape - EEDK on tape	User
Decrypting Read-type Command	- Host	The Secure Key Interface Facility automatically requests a key, provides authentication data and EEDK information if available, securely transfers and verifies the key material. The received Data Key is used by the Data Block Cipher Facility to decrypt the data block with using AES-GCM decryption and returning plaintext data blocks to the host; Optionally in Raw mode the encrypted data block may be returned to the host in encrypted form (not supported in approved configuration)	SEDK	- Plaintext data to host	User
Set Encryption Control Parameters (including Bypass Mode)	- Host - Library	Performed via Mode Select to Mode Page x'25' and Encryption Subpage X'C0'	Requested Mode Page and Subpage	None	User
Query Encryption Control Parameters (including Bypass Mode) "Show Status"	- Host - Library	Performed via Mode Sense to Mode Page x'25' and Encryption Subpage X'C0'	Requested Mode Page and Subpage	Mode Data	User

Service	Interface(s)	Description	Inputs	Outputs	Role
Drive Challenge/Response	- Host - Library	Allows programming challenge data and reading an optionally) encrypted, signed response; not used in default configuration. Performed via mode select and mode sense to Mode Page x'25' and Encryption Subpage x'D5'; not used in default configuration	Requested Mode Page and Subpage	Mode Data	User
Query Drive Certificate	- Host - Library	Allows reading of the Drive Certificate public key. Performed via mode sense to Mode Page x'25' and Encryption Subpage x'D6'; the provided certificate is signed by the IBM Tape Root CA.	Requested Mode Page and Subpage	Mode Data	User
Query dSK	- Host - Library	Allows reading of the Drive Session (Public) Key Performed via mode sense to Mode Page x'25' and Encryption Subpage X'DF'.	Requested Mode Page and Subpage	Mode Data	User
Setup SEDK structure (a protected key structure)	- Host - Library	This is the means to import a protected private key to the TS1140 drive for use in writing and encrypted tape or in order to read a previously encrypted tape. Performed via mode select to Mode Page x'25' and Encryption Subpage x'E0'. In this service, the module generates a drive session key pair. The module then sends the dSK to the key manager where it is used to create an SEDK. Then, the key manager sends the SEDK back to the module.	Requested Mode Page and Subpage	Mode Data	User

Service	Interface(s)	Description	Inputs	Outputs	Role
Query DKx(s) – active, needed, pending , entire (all)	- Host - Library	Allows the reading from the drive of DKx structures in different categories for the medium currently mounted. Performed by Mode Select commands to Mode Page x25' and various subpages.	Requested Mode Page and Subpage	Mode Data	User
Request DKx(s) Translate	- Host - Library	This status command is used when the drive has already notified the Key Manager that is has read DKx structures from a mounted, encrypted tape and needs them translated to an SEDK and returned for the drive to read the tape. The key manager issues this command to read DKx structures which the drive requires to be translated by the Key Manager and subsequently returned to the drive as an SEDK structure to enable reading of the currently active encrypted area of tape. Performed via mode sense to Mode Page x'25' and Encryption Subpage X'EE'.	Requested Mode Page and Subpage	Mode Data	User
Request DKx(s) Generate	- Host - Library	This status command is used when the drive has already notified the Key Manager that it requires new SEDK and DKx structures to process a request to write an encrypted tape. This page provides information about the type of key the drive is requesting. Performed via mode sense to Mode Page x'25' and Encryption Subpage X'EF'.	Requested Mode Page and Subpage	Mode Data	User

Service	Interface(s)	Description	Inputs	Outputs	Role
Alter DKx(s)	- Host - Library	This command is used to modify the DKx structures stored to tape and cartridge memory. The TS1140 drive will write the modified structures out to the tape and cartridge memory as directed. Performed via mode sense to Mode Page x'25' and Encryption Subpage x'E1'.	Requested Mode Page and Subpage	Mode Data	User
Drive Error Notify and Drive Error Notify Query	- Host - Library	These status responses are the means used by the drive to notify the Key Manager that an action is required, such as a Key generation or Translate, to proceed with an encrypted write or read operation. These status responses are read via Mode Sense commands to Mode Page x'25' subpage 'EF" and 'FF'.	Requested Mode Page and Subpage	Mode Data	User
Power-Up Self-Tests	- Power - Host - Library	Performs integrity and cryptographic algorithm self-tests, firmware image signature verification	None required	Failure status, if applicable	User, Crypto Officer
Configure Drive Vital Product Data (VPD) settings	- Host - Library	Allows controlling of default encryption mode and other operating parameters	From TS1140 drive operating system	Vital Product Data (VPD)	User
Key Path Check diagnostic	- Host	As documented in the TS1140 SCSI Reference	Send Diagnostic command specifying the Key Path diagnostic	Send Diagnositc command status	User
Key Zeroization	- Service Panel - Host	Zeroes all private plaintext keys in the TS1140 drive via Service Panel Or Send Diagnostic command with Diagnostic ID EFFFh, as documented in the TS1140 SCSI Reference.	Service panel buttons Or Send Diagnostic command specifying the Key Zeroization	Diagnositc command status	Crypto Officer
Firmware Load	- Host	Load new firmware to the module	New firmware	Load test indicator	Crypto Officer

3.5 Physical Security

The TS1140 drive cryptographic boundary is the drive "brick" unit. The drive brick unit is embedded in a factory supplied canister assembly. Both the drive brick unit and the canister assembly have industrial grade covers. These covers are not removed in the field in the approved configuration. The TS1140 requires no preventative maintenance, and field repair is not performed for the unit. All failing units must be sent intact to the factory for repair.

All of the drive's components are production grade.

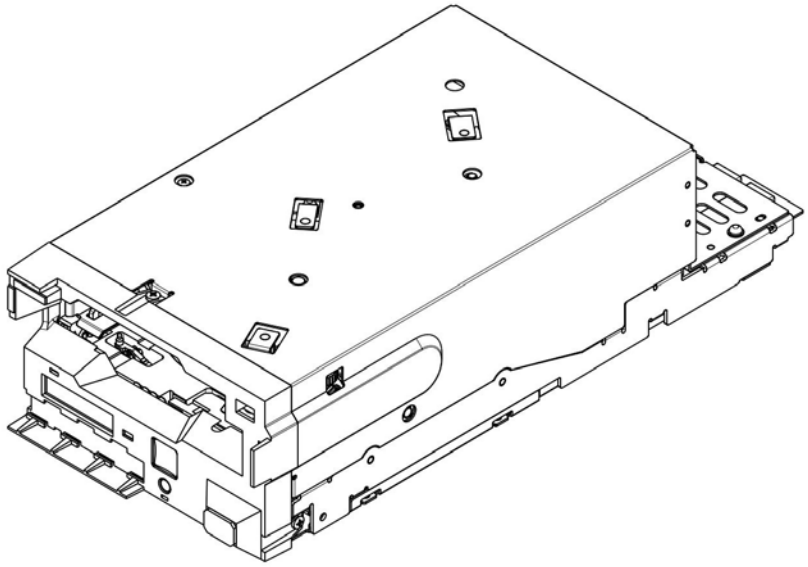


Figure 2 TS1140 Drive Brick

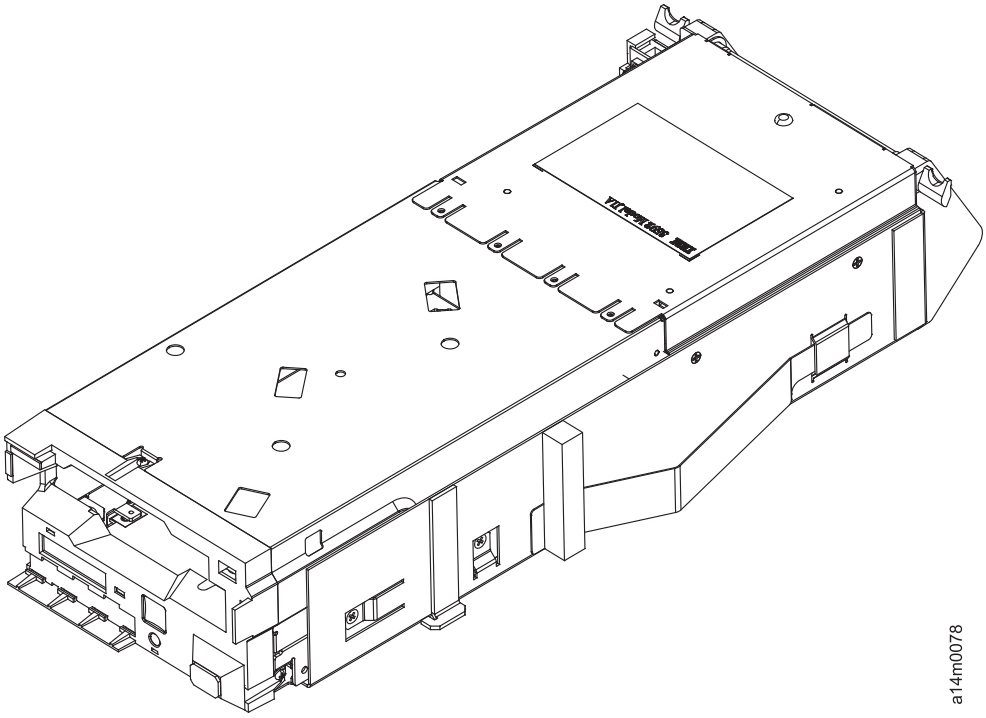


Figure 3 TS1140 Drive Canister

3.6 Cryptographic Algorithms and Key Management

3.6.1 Cryptographic Algorithms

The TS1140 drive supports the following basic cryptographic functions. These functions are used by the Secure Key Interface Facility or the Data Block Cipher Facility to provide higher level user services.

Table 6: Basic Cryptographic Functions

Algorithm	Type /Usage	Specification	Approved?	Used by	Algorithm Certificate
AES-ECB mode encryption/decryption (256-bit keys)	Symmetric cipher Provides underlying AES encryption. AES key wrapping	AES: FIPS 197	Yes	Firmware	#2385
AES-GCM mode encryption / decryption (256-bit keys)	Symmetric Cipher Encrypts data blocks while performing decrypt-on-the-fly verification Decrypts data blocks	AES: FIPS-197 GCM: SP800-38D	Yes	ASIC	#2384, #2387
DRBG	IV generation for AES-GCM, Drive Session Key generation	SP800-90 using SHA-512	Yes	Firmware	#314
SHA-1	Hashing Algorithm Multiple uses	FIPS 180-4	Yes	Firmware	#2051
SHA-256	Hashing Algorithm Digest verifies key manager messages, digest appended on messages to key manager	FIPS 180-4	Yes	Firmware	#2051
SHA-512	Hashing Algorithm Supports DRBG	FIPS 180-4	Yes	Firmware	#2051
RSA Sign/Verify	Digital signature generation and verification to sign the session key and to verify firmware image signature on firmware load	FIPS 186-2	Yes	Firmware	#1234
RSA Key Generation (2048-bit key)	Key Generation Session key generation (provides 112 bits of encryption strength)	-	No, but allowed in FIPS mode[1]	Firmware	N/A
RSA Key Transport (2048-bit key)	Decryption of transported SEDK key material (provides 112 bits of encryption strength)	-	No, but allowed in FIPS mode	Firmware	N/A

[1] Allowed for generation of keys used by the RSA Key Transport mechanism

Algorithm	Type /Usage	Specification	Approved?	Used by	Algorithm Certificate
TRNG (Custom)	Seeding DRBG	-	No[2]	ASIC	N/A

[2] Allowed in FIPS mode for seeding approved DRBG

3.6.2 Security Parameters

The following table provides a summary of both critical security parameters (CSPs) and non-critical security parameters used by the TS1140 drive.

Table 7: Security Parameters

Security Parameter	CSP	Key Type	Input into Module	Output from Module	Generation Method	Storage Location	Storage Form	Zeroized
Drive Certificate Public Key (dCert)	No	RSA 2048-bit	Yes - at time of manufacture	Yes	N/A	Drive Vital Product Data (VPD)	Non-volatile Plaintext	Yes
Drive Certificate Private Key (dCert')	Yes	RSA 2048-bit	Yes - at time of manufacture	No	N/A	Drive VPD	Non-volatile X.509 certificate signed with the IBM Tape root CA	Yes
Drive Session Public Key (dSK)	No	RSA 2048-bit	No – Generated by module	Yes	Non-approved, allowed in FIPS mode	Drive RAM	Ephemeral Plaintext	Yes
Drive Session Private Key (dSK')	Yes	RSA 2048-bit	No – Generated by module	No	Non-approved, allowed in FIPS mode	Drive RAM	Ephemeral Plaintext	Yes
Session Encrypted Data Key (SEDK)	No	RSA-2048 encrypted with the dSK	Yes	No	N/A	Drive RAM	Ephemeral Encrypted	Yes
Data Key (DK)	Yes	AES 256-bit symmetric key	Yes – (Received in encrypted form, encapsulated in the SEDK)	No	N/A	Before Use: Drive RAM	Ephemeral Plaintext	Yes
						When in use: Unreadable register in ASIC	Ephemeral Encrypted form as SEDK	
Cryptographic Data Key (cDK)	Yes	AES 256-bit symmetric key	No – Generated by module	No	DRBG	Before Use: Drive RAM	Ephemeral plaintext	Yes
DRBG Entropy Input String	Yes	256-bit input string	No – Generated by module	No	TRNG	Drive RAM	Ephemeral Plaintext	Yes
DRBG value, V	Yes	256 bits	No - Generated by module	No	Internal state value of DRBG	Drive RAM	Ephemeral Plaintext	Yes
DRBG constant, C	Yes	256 bits	No – Generated by module	No	Internal state value of DRBG	Drive RAM	Ephemeral Plaintext	Yes

Additional notes on key management:

- Secret and private keys are never output from the TS1140 drive in plaintext form.
- Secret keys may only be imported to the TS1140 drive in encrypted form.
- The module generates cryptographic keys whose strengths are modified by available entropy.
- Zeroization behavior outlined in Table 7

Table 8: CSP Access Table

	Drive Certificate Public Key (dCert)	Drive Certificate Private Key (dCert')	Drive Session Public Key (dSK)	Drive Session Private Key (dSK')	Session Encrypted Data Key (SEDK)	Data Key (DK)	Cryptographic Data Key cDK	DRBG Entropy Input Key	DRBG value , V	DRBG Constant, C
General SCSI commands										
General Library Interface commands	R		R		W					
Service Panel Configuration										
Service Panel Diagnostics					X	X	X	X	X	X
Service Panel Status Display										
Front Panel Interface Status										
Front Panel Interface Unload			W	W	W	W	W			
Front Panel Interface Reset			W	W	W	W	W	W	W	W
Encrypting Write-type Command						X	X			
Decrypting Read-type Command						X	X			
Set Encryption Control Parameters (including Bypass Mode)										
Query Encryption Control Parameters (including Bypass Mode) "Show Status"										
Drive Challenge/Response	X	X	X	X						
Query Drive Certificate	R									
Query dSK		X	R							
Setup an SEDK and EEDK structure (a protected key structure)				X	W	W	W			
Query EEDK(s) – active, needed, pending , entire (all)										
Request EEDK(s) Translate					R					
Request EEDK(s) Generate					W					
Alter EEDK(s)				X	RW					
Drive Error Notify and Drive Error Notify Query										
Power-Up Self-Tests					X	X	X	X	X	X
Configure Drive Vital Product Data (VPD) settings	W	W								
Key Path Check diagnostic	X	X	RX	X	R					
Key Zeroization	W	W	W	W	W	W	W	W	W	W
Firmware Load Test										

3.6.3 Self-Test

The TS1140 drive performs both Power On Self Tests and Conditional Self tests as follows. The operator shall power cycle the device to invoke the Power On Self tests.

Table 9: Self-Tests

Function Tested	Self-Test Type	Implementation	Failure Behavior
AES-ECB	Power-up	KAT performed for Encrypt and Decrypt	FSC[3] D131 posted
AES-GCM (256-bit keys)	Power-Up	KAT performed for Encrypt and Decrypt (256-bit)	FSC D130 posted
DRBG	Power-Up	KAT performed	Drive reboot
SHA-1	Power-Up	KAT performed	FSC D131 posted
SHA-256	Power-Up	KAT performed	FSC D131 posted
SHA-512	Power-Up	KAT performed	FSC D131 posted
RSA Sign KAT and Verify KAT	Power-Up	Separate KATs performed for sign and verify with pre-computed results	FSC D131 posted
Application Firmware Integrity Check	Power-Up	RSA digital signature verification of application firmware;	Drive reboot
VPD Integrity Check	Power-Up	CRC check of vital product data (VPD);	FSC D131 posted
DRBG	Conditional: When a random number is generated	Continuous random number generator test performed.	Drive reboot
TRNG (Custom)	Conditional: When a random number is generated	Continuous random number generator test performed.	Drive reboot
Firmware Load Check	Conditional: When new firmware is loaded	RSA signature verification of new firmware image before new image may be loaded	Code load is rejected
Exclusive Bypass Test	Conditional: When switching between encryption and bypass modes	Ensure correct data output after switching modes Check to ensure the key is properly loaded (Note: The same implementation serves as the Alternating Bypass Test.)	FSC F001 posted
Alternating Bypass Test	Conditional: When switching between encryption and bypass modes	Ensure correct data output after switching modes Check to ensure the key is properly loaded (Note: The same implementation serves as the Exclusive Bypass Test.)	FSC F001 posted
Key Path test	Conditional: When the Send Diagnostic command specifying this diagnostic number is received from the host fibre or library port; the drive must be unloaded and idle or the command is rejected	The drive will initiate a key request and key transfer operation with an attached Key Manager; random protected key material is imported into the device and checked for validity; status is reported back to the Key Manager and the invoking Host	FSC D132 posted

[3] Fault Symptom Code

3.6.4 Bypass States

The TS1140 supports the following bypass states:

Table 10: Bypass States

Bypass State	To enter the Bypass State	To verify the Bypass State
Static Bypass Mode 1: Encryption disabled	Issue a Mode Select command to mode page X'25' and set the "Encryption Disabled" bit	Issue a Mode Sense command to verify the mode is accurately reflected on mode page X'25'
Static Bypass Mode 2: Zero key usage for all records	Issue a Mode Select command to mode page X'25' and set bit 0 of Encryption Control 3 to 1	
Alternating Bypass Mode 1: Zero Key usage all labels	Issue a Mode Select command to mode page X'25' and set bit 2 of Encryption Control 3 to 1	
Alternating Bypass Mode 2: Zero Key usage on Volume Labels	Issue a Mode Select command to mode page X'25' and set bit 1 of Encryption Control 3 to 1	

Bypass entry, exit, and status features are provided to meet approved methods for use of bypass states.

3.7 Design Assurance

TS1140 drive release parts are maintained under the IBM Engineering Control (EC) system. All components are assigned a part number and EC level and may not be changed without re-release of a new part number or EC level.

The following table shows the validated configuration for each host interfaces of the TS1140 encrypting tape drive:

Table 11: Validated Configuration

Hardware EC Level	00V6759 EC Level M11776
Firmware EC Level	35P2401 EC Level M11776

3.8 Mitigation of other attacks

The TS1140 drive does not claim to mitigate other attacks.
