IBM System Storage TS1120 Tape Drive - Machine Type 3592, Model E05

Security Policy

Version 1.0 Revision 5.0

1 Document History

Date	Author	Change
02/05/2007	James Karp	Initial Creation
02/15/2007	James Karp	Added in code EC numbers
02/19/2007	James Karp	Added links to references
06/05/06	James Karp	Update supported services and configuration information
08/14/2007	Christine Knibloe	Incorporated feedback from Atlan
11/06/2007	James Karp	Incorporated additional feedback from Atlan
02/29/2008	James Karp	Reviewed and accepted additional changes from Atlan
05/01/2008	Christine Knibloe	Reviewed and accepted changes from Atlan

2 Introduction

This non-proprietary cryptographic module security policy describes how the IBM System Storage TS1120 Tape Drive - Machine Type 3592, Model E05meets the security requirements of FIPS 140-2 at overall security level 1, and how to run the TS1120 in a secure FIPS 140-2 manner. This policy was prepared as part of FIPS 140-2 validation of the TS1120. The IBM System Storage TS1120 Tape Drive - Machine Type 3592, Model E05is referred to in this document as the TS1120 Encrypting Tape Drive, the TS1120, the 3592 E05, and the encrypting tape drive.

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/cryptval/

The security policy document is organized in the following sections. Introduction

- References
- Document Organization

TS1120 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 the operations and capabilities of the TS1120 Encrypting Tape Drive only in the technical terms of FIPS 140-2 cryptographic module security policy and security functions performed by the tape drive. More information is available on the general function of the TS1120 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 TS1120 in various environments can be found at:

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

The TS1120 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://ieee-p1619.wetpaint.com/

2.2 Document Organization

The Security Policy document is one document in a complete FIPS 140-2 Submission Package. In addition to this document, the complete submission package contains:

- Vendor Evidence Document
- Other supporting documentation and additional references

With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Documentation is proprietary to IBM and is releasable only under appropriate non-disclosure agreements. For access to these documents, contact IBM.

3 TS1120 Encrypting Tape Drive Cryptographic Module Description

3.1 Overview

The TS1120 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 tape drive is FIPS certified as an entire "brick" unit as an embedded, multi-chip, cryptographic module. In customer operation the "brick" unit is embedded in a canister package for operation in a library or stand-alone frame. A block diagram of the TS1120 Encrypting Tape Drive is shown below:

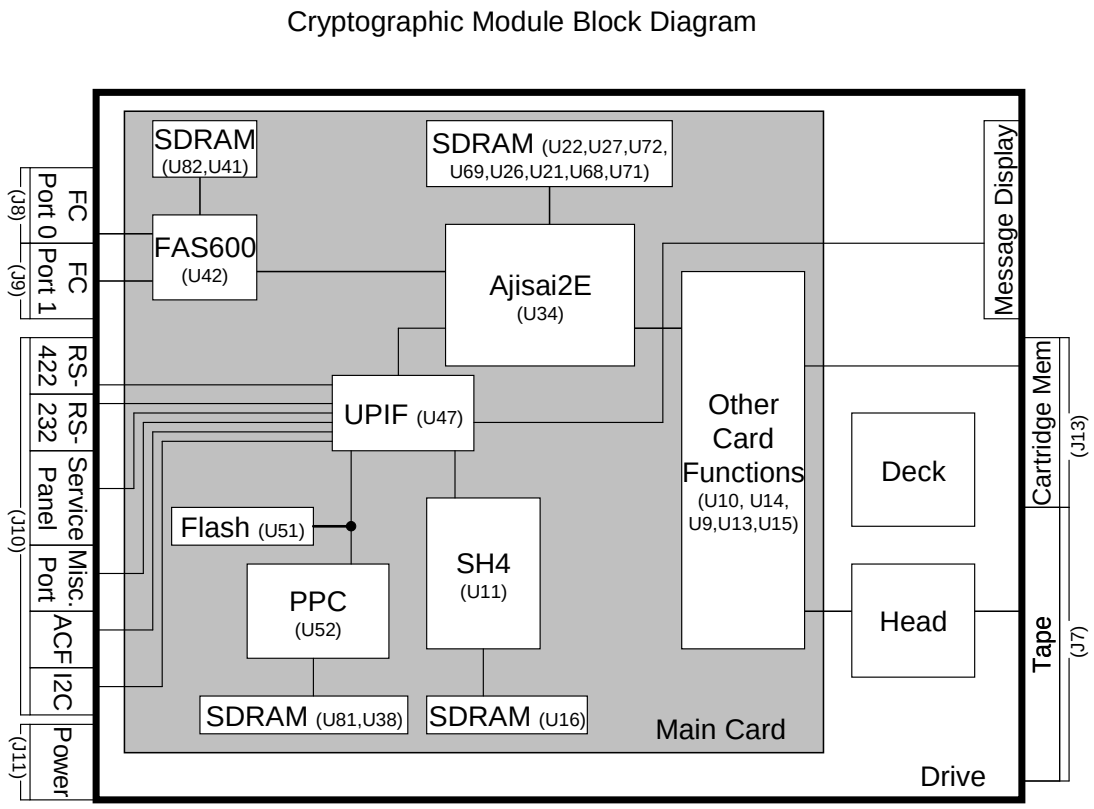


Figure 1 : TS1120 Block Diagram

The TS1120 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 block cipher using a provided key, and decrypted during reads from tape using a provided key .
  - Note the AES block cipher operation is performed after compression of the host data therefore not impacting capacity and datarate performance of the compression function
  - The TS1120 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, (referred to in this document as the EKM), and allow establishment of encrypted key material between the key manager and the tape drive

3.2 Secure Configuration

There are two approved modes of operation for the TS1120. They are:
- System-Managed Encryption (SME)
- Library-Managed Encryption (LME)

A user may select an approved mode of operation by two different methods. The first is configuring the drive's VPD. This can be accomplished via the service panel interface or the library interface. The second method is issuing a SCSI Mode Select command to set values in Mode Page X'25'.

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 TS1120 SCSI Reference.

Table 6.1: Settings for Approved Modes of Operation

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	X'1'	X'6'
In-band Key Path (Manager Type) Override Mode Page X'25', byte 21, bits 4-2	X'0' or X'1'	X'0'
Indirect Key Mode Default Mode Page X'25', byte 22, bit 4	B'0'	B'0'
Key Scope Mode Page X'25', byte 23, bits 2-0	X'0' or X'1'	X'0' or X'1'
Encryption Method Mode Page X'25', byte 27	X'10' or X'1F'	X'60'

A user can determine if the TS1120 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 modes of operation. The commands vary by approved mode. In the LME approved mode of operation, all Mode Select commands to subpages of Mode Page X'25' are prohibited. In the SME approved mode of operation, Mode Select commands to the following subpages of Mode Page X'25' are prohibited.

Table 6.2: Mode Select Eligibility of Mode Page X'25' Subpages

Mode Page X'25' Subpages	System-Managed Encryption (SME)	Library-Managed Encryption (LME)
X'C0' – Control/Status	**Allowed**	Prohibited
X'D0' – Generate dAK/dAK' Pair	Prohibited	Prohibited
X'D1' – Query dAK	Prohibited	Prohibited
X'D2' – Update dAK/dAK' Pair	Prohibited	Prohibited
X'D3' – Remove dAK/dAK' Pair	Prohibited	Prohibited
X'D5' – Drive Challenge/Response	**Allowed**	Prohibited
X'D6' – Query Drive Certificate	**Allowed**	Prohibited
X'D7' – Query/Setup HMAC	Prohibited	Prohibited
X'D8' – Install eAK	Prohibited	Prohibited
X'D9' – Query eAK	Prohibited	Prohibited
X'DA' – Update eAK	Prohibited	Prohibited
X'DB' – Remove eAK	Prohibited	Prohibited
X'DF' – Query dSK	**Allowed**	Prohibited
X'E0' – Setup SEDK/EEDK(s)	**Allowed**	Prohibited
X'E1' – Alter EEDK(s)	**Allowed**	Prohibited
X'E2' – Query EEDKs (Active)	**Allowed**	Prohibited
X'E3' – Query EEDKs (Needed)	**Allowed**	Prohibited
X'E4' – Query EEDKs (Entire)	**Allowed**	Prohibited
X'E5' – Query EEDKs (Pending)	**Allowed**	Prohibited
X'EE' – Request EEDKs (Translate)	**Allowed**	Prohibited
X'EF' – Request EEDKs (Generate)	**Allowed**	Prohibited
X'FE' – Drive Error Notify	**Allowed**	Prohibited

Loading a FIPS-certified drive microcode level and selecting an approved mode of operation initializes the TS1120.

The TS1120 supports multi-initiator environments, but only one initiator may access cryptographic functions at any given time. Therefore the TS1120 does not support multiple concurrent operators.

The TS1120 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.

3.3 Ports and Interfaces

The cryptographic boundary of the TS1120 cryptographic module is the drive “brick” boundary and therefore supports all the interfaces of a standard tape drive. Tape data blocks to be encrypted (write operations) or decrypted data blocks to be returned to the host (read operation) are transferred on the Fibre Channel ports using SCSI protocol commands, while protected key material may be received on the Fibre Ports or the Library Port.

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

Table 1 : Ports and Interfaces

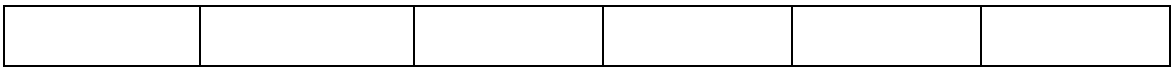
TS1120 Physical Interface	FIPS-140-2 Logical Interface	Notes
Fiber Channel Port 0	Data Input Data Output Control Input Status Output	Provides crypto service
Fiber Channel Port 1	Data Input Data Output Control Input Status Output	Provides crypto services
Library RS-422 Port	Data Input Data Output Control Input Status Output	Provides crypto services
Drive RS-232 Port	None (Disabled)	No services provided
ACF interface	Status Output Control Input	No crypto services provided
I2C Interface	Status Output Data Output Data Input Control Input	No crypto services provided
Miscellaneous Signal Interface	None	Spare and unused signals

TS1120 Physical Interface	FIPS-140-2 Logical Interface	Notes
Service Panel Interface	Control Input Status Output	Crypto services provided: Crypto status (encrypting or not) posted to message display Key zeroization VPD configuration
Drive Message Display	Status Output Control Input (reset / unload button)	Crypto services provided: Crypto status (encrypting or not) posted to message display
Drive Power Interface	Power	No crypto services provided
RW Head Interface	Data Output Data Input	No Crypto services provided: Encrypted data is recorded to media or readback from media on this interface
Cartridge Memory Interface	Data Output Data Input	No Crypto services provided: Encrypted key structures may be written to the cartridge memory or read from the cartridge memory on this interface

3.3.1 Interface Description

- Fibre Channel Port 0 and 1
  - Host attachment interfaces accepting SSC-3 SCSI protocol commands and status
  - Raw and encrypted data blocks and encrypted keys are transferred on this interface
- Library RS-422 port
  - Automation interface using LDI or LMI command and status protocol
  - Encrypted key material may be transferred on this interface
- Drive RS-232 port
  - Debug port proprietary protocol
  - This interface is disabled in FIPS configuration – no function available

- ACF interface
  - Memory-mapped interface with extended processor data and address bus
  - Used to communicate to external logic on the canister and library
  - Drive is the interface master – no services provided
- I2C Interface
  - Standard 2-wire I2C control and status interface
  - Used to monitor external power supply status and to R/W external backup VPD
  - Drive is interface master – no services provided
- Miscellaneous Signal Interface
  - Unused spare signals wired to the connector
- Service Panel Interface
  - Used to attach an external Service Panel for configuration and status services
  - Power is supplied by the module to the external service panel on this interface
- Drive Message Display
  - Physical operator interface
  - Provides 8 character display, unload button, reset button
- Drive Power Interface
  - DC power interface providing +12V, +5V, ground
- RW Head Interface
  - Magnetic interface from the R/W head to the tape media
  - Used to magnetically record signals to the tape on writing and magnetically read signals on read back
- Cartridge Memory Interface
  - Each tape cartridge contains a small cartridge memory which stores status information about the tape cartridge
  - This is a contactless short distance RFID serial transmit/receive protocol interface



3.3.2 Roles and Services

The TS1120 supports both a Crypto Officer Role and a User Role, and uses basic cryptographic functions to provide higher level services. The two main services the TS1120 provides are:

- the encryption or decryption of tape data blocks using the Data Block Cipher Facility.
- the 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 TS1120. Under these circumstances the TS1120 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.

3.3.3 User Guidance

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

- There is no requirement for accessing the User Role
- To access the Crypto Officer role, a Service Panel must be attached and the TS1120 must be placed in the CE Offline state. This disables all interfaces with the exception of the service panel.

Single Operator requirements:

- The TS1120 enforces a requirement that only one host fiber channel Initiator may have access to cryptographic services at any given time.

3.3.4 Provided Services

Available services are also documented in the specified references. They are summarized here:

Service	**Available on :**	**Description**	**Role**	**Access to Keys/CSPs**
General purpose and vendor unique SCSI SSC-3 commands	Fiber Channel Port 0 Fiber Channel Port 1	As documented in the TS1120 SCSI Reference	User	None
General purpose library commands	Library RS-422 Interface	As documented in the Drive Library LDI and LMI Interface Specifications	**User**	**None**
Drive Service Panel Configuration , Diagnostic and Status services	Service Panel	Services are provided for Configuration, Diagnostic, and Status. The services are performed manually with control button sequences on an attachable Service Panel as documented in 3592 E05 Maintenance Information Manual	**User**	**None**

Service	Available on :	Description	Role	Access to Keys/CSPs
Drive Message Display services	Drive Message Display	The drive services provided by the message display consist of: ▪ Unload button - drive will unload when pressed ▪ Reset Button – drive will reset when pressed	**User**	**None**
Write Command (SCSI command x‘0A’) (with encryption enabled)	Fiber Port 0 Fiber Port 1	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 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 decryption of the encrypted data block and verifies the correctness of the encryption process	User	Uses DK
Read Command (SCSI command x’08’) (with encryption enabled)	Fiber Port 0 Fiber Port 1	The Secure Key Interface Facility automatically requests a key, provides authentication data and EEDK wrapped key 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 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)	User	Uses DK
Access to Encryption Control registers for program control	Fiber Port 0 Fiber Port 1 Library Interface	Performed via mode select to Mode Page x’25’ and Encryption Subpage x’C0’	User	None

Service	Available on :	Description	Role	Access to Keys/CSPs
Access to Encryption Status registers for program status monitoring	Fiber Port 0 Fiber Port 1 Library Interface	Performed via mode sense to Mode Page x'25' and Encryption Subpage x'C0'	User	None
Query Drive Certificate	Fiber Port 0 Fiber Port 1 Library Interface	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.	User	Reads dCert
Query dSK	Fiber Port 0 Fiber Port 1 Library Interface	Allows reading of the Drive Session (Public) Key Performed via mode sense to Mode Page x'25' and Encryption Subpage x'DF'.	User	Reads dSK
Setup an SEDK and EEDK structure (a protected key structure)	Fiber Port 0 Fiber Port 1 Library Interface	This is the means to import an encrypted private key to the TS1120 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 EKM where it is used to create an SEDK. At this time, the EKM also uses its own RSA key to generate the EEDK. Then, the EKM sends both the SEDK and the EEDK back to the module.	User	Uses SEDK, dCert, & dSK. generates dSK.
Query EEDK(s) – active, needed, pending , entire (all)	Fiber Port 0 Fiber Port 1 Library Interface	Allows the reading from the drive of EEDK structures in different categories for the medium currently mounted. Performed by Mode Select commands to Mode Page x25' and various subpages.	User	None

Service	Available on :	Description	Role	Access to Keys/CSPs
Request EEDK(s) Translate	Fiber Port 0 Fiber Port 1 Library Interface	This status command is used when the drive has already notified the Key Manager that it has read EEDKs 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 EEDK(s) 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' .	User	Users dSK, dCert, & SEDK
Request EEDK(s) Generate	Fiber Port 0 Fiber Port 1 Library Interface	This status command is used when the drive has already notified the Key Manager that it requires new SEDK and EEDK(s) 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' .	User	Uses dSK, dCert, SEDK
Alter EEDK(s)	Fiber Port 0 Fiber Port 1 Library Interface	This command is used to modify the EEDK structures stored to tape and cartridge memory. The TS1120 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' .	User	None
Drive Error Notify and Drive Error Notify Query	Fiber Port 0 Fiber Port 1 Library Interface	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'.	User	None
Power On Self-Tests	Power	Performs integrity and cryptographic algorithm self-tests, code image signature verification	User	None

Service	Available on :	Description	Role	Access to Keys/CSPs
Configure Drive VPD settings	Fiber Port 0 Fiber Port 1 Library Interface Service Panel	Allows controlling of default encryption mode and other operating parameters	User	None
Diagnostic Program Invocation	Fiber Port 0 Fiber Port 1 Service Panel	A Send Diagnostic command may be issued on Fiber or library interfaces to invoke diagnostics. The only supported crypto diagnostic from this interface is the Key Path Check diagnostic. The user must power cycle the drive to invoke full self-test diagnostics	User	None
Firmware Upgrade	Fiber Port 0 Fiber Port 1	Attempts to load a new, signed version of the drive firmware. The drive will only load signed firmware after first verifying its integrity and authenticity.	User	None
Key Zeroization	Service Panel	Zeroes all private plaintext keys in the TS1120	Crypto Officer	None

3.4 Physical Security

The TS1120 is intended to meet level one physical security requirements. The TS1120 cryptographic boundary is the drive "brick" unit. The drive brick unit has industrial grade covers, and all the drive's components are production grade. The TS1120 drive requires no preventative maintenance, and field repair is not performed for the unit. The drive brick covers are not removed in the field in the approved configuration. All failing units must be sent intact in the canister to the factory for repair.

The brick unit is embedded in a (factory supplied) canister assembly that also has industrial grade covers. The figures below show the TS1120 drive brick and canister.

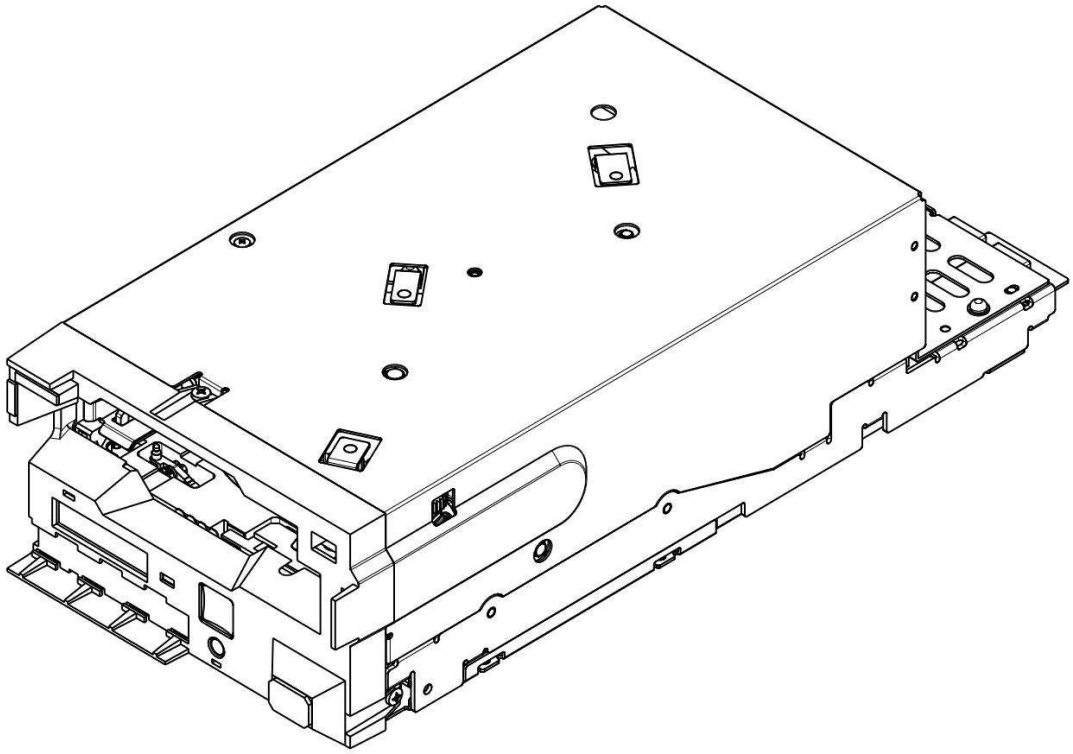


Figure TS1120 Drive Brick

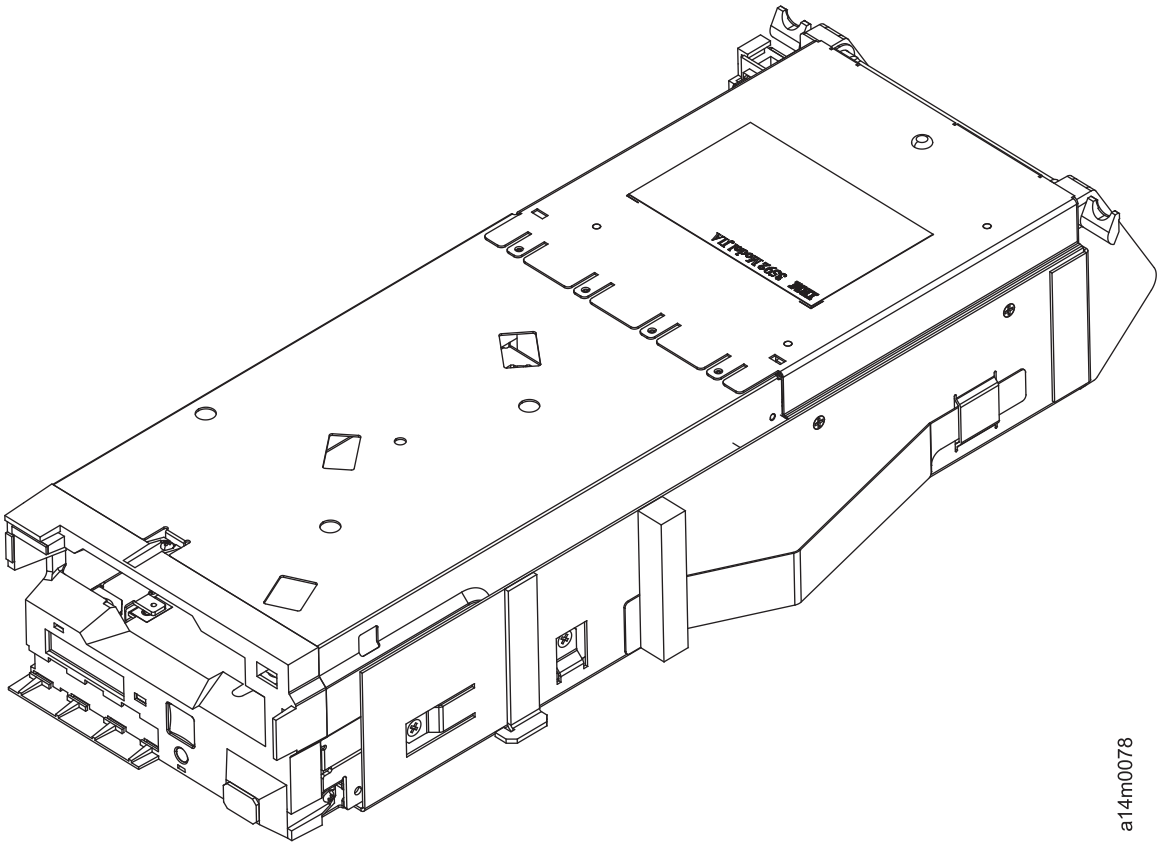


Figure 2 TS1120 Drive Canister

3.5 Cryptographic Algorithms and Key Management

3.5.1 Cryptographic Algorithms

The TS1120 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 2 : Basic Cryptographic Functions

Algorithm	Type /Usage	Specification / Approved	Performed by/Used by
AES mode encryption / decryption (256-bit keys)	Symmetric Cipher Encrypts data blocks while performing decrypt-on-the-fly verification Decrypts data blocks	AES FIPS-197 underlying AES	ASIC

Algorithm	Type /Usage	Specification / Approved	Performed by/Used by
PRNG	IV generation for AES counter mode, Drive Session Key generation	X-FIPS 186-2 (original) SHA-1 based	Code
SHA-1	Hashing Algorithm Multiple uses	FIPS-180-2	Code Used in PRNG and other internal operations
SHA-256	Hashing Algorithm Digest checked on EKM messages, digest appended on messages to EKM	FIPS-180-2	Code
RSA Key Establishment	RSA Key Generation ▪ Session key generation ▪ 2048-bit key Decryption ▪ Decryption of transported key material ▪ SEDK decrypt	Non-approved, but allowed in FIPS mode	Code
RSA PKCS#1-v1.5 RSASSA-PKCS1-v1_5.	Digital signature signing and verification ▪ Used to sign the session key with the dCert' ▪ Verifies code image signature before use on new code image load	FIPS-186-2	Code
TRNG (Custom)	Seeding PRNG	Non-Approved	ASIC

3.5.2 Keys and CSPs

Key usage and flows are outlined in the Tape Drive Design and Key Flow documentation. This is a summary of CSPs and other keys used by the TS1120.

Cryptographic Key (CSP)	Key Type	Generation	Approved Generation	Entered into device	Output from device	Storage/Form	Zeroization
Drive Certificate Public Key	RSA 2048-bit PKCS#1 (at time of manufacture, not generated by drive)	No	N/A	Yes at time of manufacture	Yes (upon request)	Drive VPD Non-volatile Plaintext	N/A
Drive Certificate Private Key dCert' CSP	RSA 2048-bit PKCS#1 (at time of manufacture, not generated by drive)	No	N/A	Yes at time of manufacture	No	Drive VPD Non-volatile Obfuscated Plaintext	Yes
Drive Session Public Key dSK	RSA 2048-bit PKCS#1	Yes	No (allowed in FIPS mode)	No	Yes (upon request)	Drive RAM Ephemeral Plaintext	N/A
Drive Session Private Key dSK' CSP	RSA 2048-bit PKCS#1	Yes	No (allowed in FIPS mode)	No	No	Drive RAM Ephemeral Obfuscated Plaintext	Yes
186-2 PRNG Key CSP	Seed (20 bytes)	Yes	Yes (using TRNG)	No	No	Drive RAM Ephemeral Plaintext	Yes
186-2 PRNG Seed	Seed (20 bytes)	Yes	Yes (using TRNG)	No	No	Drive RAM Ephemeral Plaintext	Yes
IV Random Number	Number used to form nonce for AES counter blocks, 16 bytes	Yes	Yes (using PRNG)	No	No	Drive RAM Ephemeral Plaintext	Yes

Cryptographic Key (CSP)	Key Type	Generation	Approved Generation	Entered into device	Output from device	Storage/Form	Zeroization
Session Encrypted Data Key SEDK	AES-256 Data Key that is received in encrypted form from the EKM ; RSA-2048 encrypted with the Drive Session Public Key	No	N/A	Yes, encrypted through RSA key transport	No	Drive RAM Ephemeral (Transiently) Stored in its received, RSA encrypted form	Yes
Externally Encrypted Data Key EEDK (not a CSP)	AES-256 Data Key that is received in an encrypted form from the EKM, which only the EKM can decrypt	No	N/A	Yes encrypted	Yes (upon request and to tape cartridge and CM port)	Drive RAM Ephemeral Stored in its received, encrypted form	N/A
Data Key DK CSP	AES-256 bit symmetric key	No	N/A	Yes (as SEDK only) (encrypted)	No	When in use: Stored In ASIC; (unreadable register) Ephemeral Plaintext Before Use: Drive RAM Ephemeral Encrypted form as SEDK After use: Zeroized	Yes
Firmware Image Certificate	RSA 2048 bit public key	No	N/A	No	No	Hard Coded	No

Additional notes on key management:

- Private key material is never output from the TS1120 in plaintext, only in encrypted form
- Private key material may only be imported to the TS1120 in encrypted form

3.5.3 Bypass States

The TS1120 supports the following bypass states:

- Static Bypass Mode 1: Encryption disabled
- Static Bypass Mode 2: Zero key usage for all records
- Alternating Bypass Mode 1: Zero Key usage all labels
- Alternating Bypass Mode 2 : Zero Key usage on Volume Labels

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

3.5.4 Self-Test

The TS1120 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.

Algorithm	Power on Self Test
AES (256-bit keys)	KAT performed for Encrypt and Decrypt (256-bit)
PRNG	KAT performed
SHA-1	KAT performed
SHA-256	KAT performed
PKCS #1 :RSA Key Generation (1024/2048-bit keys)	No KAT test required; Continuous self-test performed
PKCS #1 RSA Encryption/Decryption (1024/2048-bit keys)	No KAT required, but internal self test is performed
TRNG (Custom)	No KAT required
Software/Firmware Integrity Check	Yes CRC check of all images on reboot;

Conditional self tests are also performed by the TS1120 as follows:

Function	Conditional self test	Condition	Implementation
PRNG	Yes	Every time a random number is generated	Ensure the newly generated random number does not match the previously generated random number . Also ensure the first number generated after start up is not used and is stored for the next comparison
SHA-1	No	N/A	N/A
SHA-256	No	N/A	N/A
PKCS #1 :RSA Key Generation (1024/2048-bit keys)	Yes	When a new key is generated	Ensure that the new key pair is valid, perform sign/verify including PKCS#1 formatting and SHA-1 hashing
PKCS #1 RSA Encryption/Decryption (1024/2048-bit keys)	No	N/A	N/A
TRNG (Custom)	Yes	Every time a random number is generated	Ensure the newly generated random number does not match the previously generated random number . Also ensure the first number generated after start up is not used and is stored for the next comparison
Software/Firmware Load Test (drive firmware)	Yes	Every time new firmware is loaded	RSA PKCS #1 signature verification of new code image before new image may be loaded
Seed and Seed key check	No	When seeding or re-seeding an approved PRNG; TRNG is used for this purpose. (See TRNG conditional self-test.)	Ensure that the XSeed and XKey values are not equal for FIPS 186-2 generation. XKey and XSeed are generated from the hardware TRNG, and compared on instantiation of the PRNGs. If XKey is equal to XSeed then they are regenerated until not equal.

Function	Conditional self test	Condition	Implementation
Exclusive Crypto Bypass Test and Alternating Crypto Bypass-Test (note: the same checks serve as both alternating and exclusive bypass tests)	Yes	When switching between encryption and bypass modes	Ensure the correct output of data after switching modes, and ensure that no change to the bypass state has been made since the last official switch.
Key Path test	Yes	When the Send Diagnostic command specifying this diagnostic number is received from the host fiber 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

3.6 Design Assurance

TS1120 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 certified TS1120 hardware level is :

Part Number 23R6564 EC level H82149.

The certified drive firmware level is:

EC H82669

95P5202 CD Rom

95P5203 Microcode Image

95P5204FRU: CD Rom (includes the paper envelope)

3.7 Mitigation of other attacks

The TS1120 does not claim to mitigate other attacks.