CryptoStor Tape 702/704
Security Policy
Non-Proprietary

FC702 P/N 820-0004-01 Rev 2 FW: Rev 2.1.0
FC704 P/N 820-0005-01 Rev 1 FW: Rev 2.1.0

NeoScale Systems, Inc.

January 9, 2006
Document Revision 0.8

TABLE OF CONTENTS

Document History

Rev	Comments	Author	Date
0.1	Initial draft	H. Puri	12/31/04
0.2	Changed name to 700 Series	H. Puri	02/18/05
0.3	Incorporated feedback	D. Shah	5/3/2005
0.4	More changes based on feedback	D. Shah	5/22/2005
0.5	Final changes	D. Shah	6/8/2005
0.6	Added SHA-512 Certificate Number	D. Shah	6/17/2005
0.7	Updated to reflect comments from NIST/CSE	Rose Quijano-Nguyen	11/16/2005
0.8	Additional requirements from NIST/CSE	Rose Quijano-Nguyen	01/09/06

Acronyms and Abbreviations

AES	Advanced Encryption Standard
CLI	Command Line Interface
CM	Cryptographic Module
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
DES	Data Encryption Standard
FIPS	Federal Information Processing Standard
GUI	Graphical User Interface
LUN	Logical Unit Number
NIST	National Institute of Standards and Technology
RNG	Random Number Generator
SAN	Storage Area Network
UI	User Interface

Introduction

Purpose

This is a non-proprietary Cryptographic Module Security policy for the CryptoStor Tape 700 Series from NeoScale Systems, Inc. This security policy describes how the CryptoStor Tape 700 Series SAN Security Appliances meet the security requirements of FIPS 140-2 and how to run the module in an approved mode of operation. This document was prepared as part of the Level 3 FIPS 140-2 validation of the Tape 700 Series.

References

This document provides information on the security operations and capabilities of the Tape 700 Series as it relates to FIPS 140-2. More information is available on the Tape 700 Series from the NeoScale Systems website at http://www.neoscale.com.

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 website at http://csrc.nist.gov/cryptval/.

Security Level

The CryptoStor Tape 700 Series is designed to comply with the overall requirements of FIPS 140-2, level 3. The following table indicates module level compliance as applicable:

Security Requirements Section	Level
Cryptographic Module Specification	3
Cryptographic Module Ports & Interfaces	3
Roles, Services and Authentication	3
Finite State Model	3
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self-Tests	3
Design Assurance	3
Mitigation of Other Attacks	N/A
Cryptographic Module Security Policy	3
Overall Level of Certification	3

The CryptoStor Tape 700 Series does not contain a user accessible operating system nor provide services for mitigation of other forms of attack aside from those specified.

Overview

The NeoScale CryptoStor FC702 and FC704 appliances, referred to in this document as the Tape 700 Series, are Fibre Channel Storage Area Network (SAN) data security appliances that provide encryption for tape media based on configured policy rules. Operating as a fully transparent, in-line storage appliance, the Tape 700 Series inspects backup traffic and applies strong encryption to the data payload at gigabit rates. Backup data privacy policies are centrally managed, employing encryption rules which are easily modified to suit current and evolving storage infrastructures. True gigabit throughput with low latency and transparent operation ensures uninterrupted, scalable storage data protection.

The Tape 700 Series is a multi-chip standalone module and the cryptographic boundary of the module is defined by its metal enclosure, excluding the fan and power supply assemblies which are field replaceable (hot swappable) modules. The power supply and fan ports are protected by the baffles designed to prevent probing by an attacker.

Tape 700 Series Interfaces

The Tape 700 Series provides a number of physical and logical interfaces to the device. The physical interfaces provided by the Tape 700 Series are mapped to the FIPS 140-2 defined logical interfaces: data input, data output, control input, status output as described in the following table:

Logical Interface	Physical Interface Mapping
Data Input Interface	Fibre Channel Port
Data Output Interface	Fibre Channel Port
Control Input Interface	10/100/1G BASE-TX LAN Port, Console Port; Smartcard connector
Status Output Interface	LEDs, 10/100/1G BASE-TX LAN port, Console Port, Front Panel Display; Smartcard connector
Power Interface	PCI Compact Power Connector

Table 1 – FIPS 140-2 Logical Interfaces

Currently, the Tape 700 Series consists of 2 systems: FC702 and FC704. The FC702 system has two Fibre Channel ports and two encryption cards. The FC704 system has four Fibre Channel ports and four encryption cards.

Roles and Services

The Tape 700 Series supports identity-based authentication. Users authorized to access the unit are required to enter a username and password to authenticate their identity to the system in order to perform authorized tasks. The Tape 700 Series can be accessed in one of the following ways:

- CLI via the Console Serial Port
- CLI via SSH (v2)
- Graphical User Interface (GUI) using HTTPS via TLS (SSL v3.1)

When the user successfully logs into the unit, the authorized role is allowed. The user is not allowed to alter the role while logged into the unit. Identification (user ID) and authentication (valid password) is required for accessing the unit through the serially attached administrator console. Administrators of the unit choose their own passwords and create the user-IDs for security and recovery officers. The security officer and the recovery officer will then choose their passwords. The system enforces the following passwords security policy:

- Passwords must be at least 8 characters long
- Passwords must be a mix of at least two out of three of (letters, digits, control chars)
- Three login failures via the web interface will lock out the account

Authentication of Strength

Assuming the worst case scenario where a user chooses the minimum number of characters meeting the password policy, the number of password permutations with 8 characters selected from a possible of:

52 alpha characters (upper and lower)

10 digits

\+ 10 special characters

---

72 possibilities

For every given choice, we have:

72^8 = (72*72*72*72*72*72*72*72) = **722,204,136,308,736** total permutations.

For login attempts from a remote location, the authentication mechanism is designed with an account locking feature where three consecutive login failures for a given user ID will lockout access to that user. The account will be unlocked only when the administrator unlocks it. The locking feature does not apply to administrator privileged login failures through the console. Hostile attack through the console using an administrator account provides better chances for a malicious agent trying to brute force an authentication. Although, the system does not lockout administrator login failures through the console, it imposes a delay of 5 seconds after the third failed attempt. This means, the hostile agent can at most attempt 3600 password entries (3 * 20 * 60) every hour. On average, an attacker would have to enter (722,204,136,308,736 / 2 =) **361,102,068,154,368** passwords, over (361,102,068,154,368 / 3600) **100306130042.88** hours, before entering the correct password. The average successful attack would, as a result, occur in slightly less than:

(100306130042.88 / 24 / 365 =) **1450471** years

The elapse time of attack (1450471 years) is not practical under any circumstances.

The module supports four roles by default. These are mapped as shown below:

Role	***FIPS Mapping***	***Type of Authentication***	***Authentication Data***
Administrator	Crypto-Officer	Identity-based	The operator is granted access to the Tape 700 Series CLI or GUI after providing proper user ID and corresponding password.
Security Officer	Crypto-Officer	Identity-based	The operator is granted access to the Tape 700 Series CLI or GUI after providing proper user ID and corresponding password.
Recovery Officer	Crypto-Officer	Identity-based	The operator is granted access to the Tape 700 Series CLI or GUI after providing proper user ID and corresponding password.
Super User	Crypto-Officer	Identity-based	The operator is granted access to the Tape 700 Series CLI or GUI after providing proper user ID and corresponding password.

The user accounts created by the Administrator Role are other Administrator Accounts that are able to perform the Administrator Role, Security Officer Accounts that are able to perform the Security Officer Role, and Recovery Officer Accounts that are able to perform the Recovery Officer Role. Each of these roles is described and discussed below.

Administrator Role

The Administrator is responsible for configuring the non-security services of the Tape 700 Series.

Typical functions allowed to an Administrator are:

- Unit connectivity to the SAN
- IP/LAN connectivity for UI
- CryptoStor network configuration management
- System event logging and tracking
- CryptoStor account creation, maintenance, and deletion

Security Officer Role

The Security Officer is responsible the security related aspects of the Tape 700 Series such as the implementation and management of security policies and system key management.

Typical functions allowed to a Security Officer are:

- Security Officer and Recovery Officer account management
- Data security planning and threat assessment
- Security policy rule design, configuration and maintenance
- Insertion of system keys
- Certificate maintenance and updates
- Audit log maintenance

Recovery Officer Role

The Recovery Officer is responsible for retaining a segment of the system keys required for key recovery. Multiple Recovery Officer users are required to reconstitute the system keys. Multiple Recovery Officer users are the entities that hold the other segments of the system keys.

The only task associated with the Recovery Officer is the retention of a segment of the system key.

Super User Role

This is a role that is created by combining the privileges of *Administrator*, *Security Officer* and *Recovery Officer* roles. The user thus created will be authorized to perform all the services mentioned above for these three roles.

Services

The Tape 700 Series supports the services for each role as listed in the following table. The type of access is specified as “R” for read only, “W” for write access and “E” for the ability to execute the service.

Role	Authorized Services	Cryptographic Keys and CSPs	Type(s) of Access
Administrator	View system configuration and status	None	R
	Set/modify system configuration	None	W
	Create/modify/delete user account	None	W
	Change own password	Password	W
	View system log file	None	R
	Export system log file	Key Encrypting Key (KEK)	E
	Restart system	None	E
	Firmware update	Firmware Load Key	E
Security Officer	Modify Security Officer Account	None	R, W
	Encryption/Decryption	Encryption Key	E
	Create/Zeroize system keys	Key Encrypting Key (KEK)	W, E
	Create recovery system key shares	Key Encrypting Key (KEK)	W, E
	Create/delete/ encryption keys	Encryption key	W, E
	Create/modify/delete/ volume pools	Configuration file	W
	Export catalogs	Key Encrypting Key (KEK)	E
	Zeroize keys	None	E
	Create/modify/delete security policies	Configuration file	W
	View system & audit log	None	R
	Export system & audit log files	Key Encrypting	E

Role	***Authorized Services***	***Cryptographic Keys and CSPs***	***Type(s) of Access***
		Key (KEK)	
	Change own password	Password	W
	View/import certificates	None	R, W
Recovery Officer	Export/import recovery system key share	Key Encrypting Key (KEK)	R, W
	Change own password	Password	W
Super User	All the services performed by the ***Administrator***, ***Security Officer*** and ***Recovery Officer*** roles.		

Security Functions

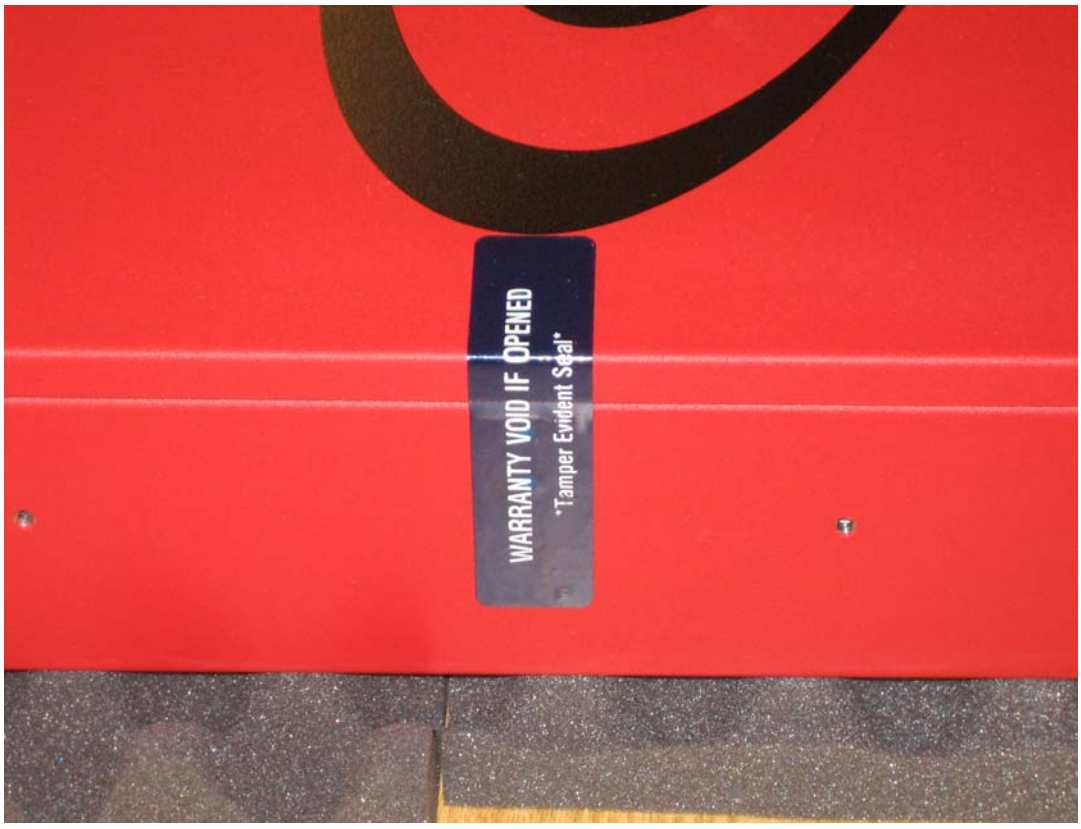
Physical Security

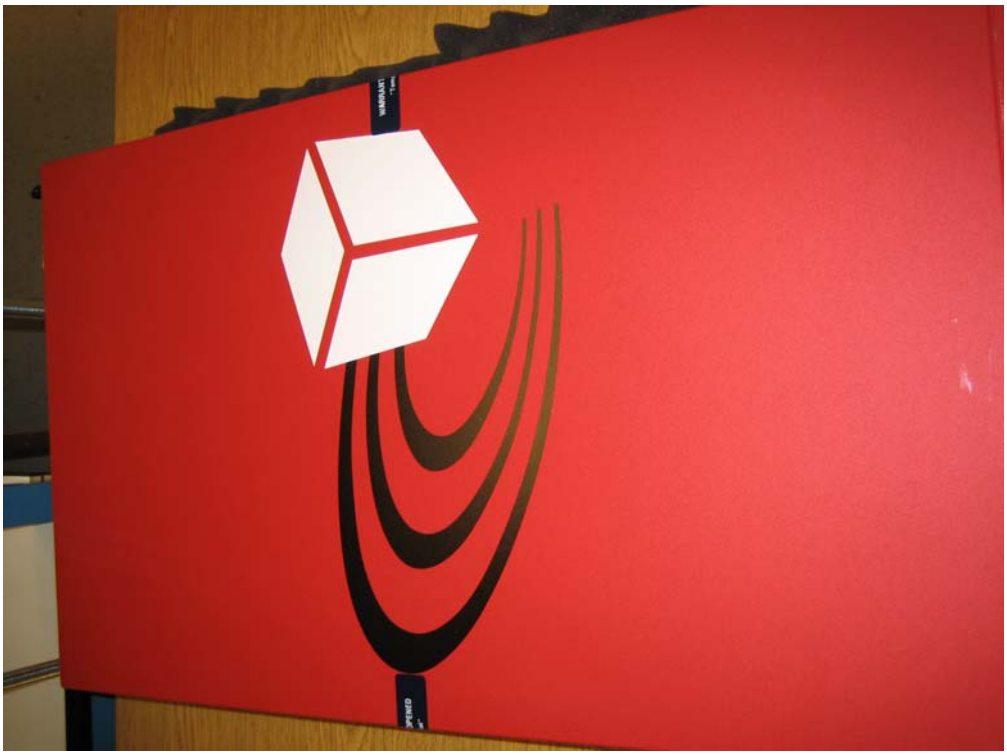
The CryptoStor Tape 700 Series is a multi-chip standalone cryptographic module designed to meet FIPS 140-2, level 3 for physical security. The module consists of production grade components with standard passivation techniques applied.

The cryptographic security boundary is defined by the unit's opaque sheetmetal enclosure with the exception of the fan and power supply modules which are field replaceable. Access to the circuitry is restricted through the use of tamper-evidence labels applied to the removable cover and chassis showing visible evidence if the unit has been opened after shipment. Tamper response and zeroization circuitry is also present to destroy plaintext CSPs upon removal of the cover.

The Tape 700 Series is 2U (3.75 inches) high by 17 inches wide by 30 inches deep. It includes a single access cover protected with the tamper-evident labels and tamper response and zeroization circuitry. The unit contains a motherboard with multiple PCI cards for fiber optic interface and encryption services. Other printed circuit boards include an interface board providing LED circuitry, a controller board, and a backplane that provides a hot swappable interface to the fan modules. Interconnect between printed circuit board assemblies is handled both through card edge connectors and cable assemblies. There is also a hard disk that stores the software image. The 2 redundant power supplies are externally accessible from the rear of the module. Power is brought to the PCBs and hard disk through a harness located at the rear of the power supply cavity which connects directly to the PCBs. Cooling for the Tape 700 Series is provided by 4 fans mounted external to the front of the main sheet metal enclosure. These fans blow air into the module with ventilation holes on the opposite side of the chassis. Ventilation holes in the housing are protected from undetected probing through the use of internal baffles.

The following screen shots 1 illustrate where to place tamper seal evidence. One tamper seal is placed in middle left corner of 702/704 and the other tamper seal is placed middle right corner. Each tamper seal sits on top or cover a screw. The only way to get to the cover is to break the tamper seals


WARRANTY VOID IF OPENED
Tamper Evident Seal



Cryptographic Key Management

- Symmetric Key Algorithms

Algorithm	Modes Implemented	Use	Key Sizes	Certificate #
TDES (FIPS 46-3)	CBC	Encryption of media Encryption of log files	168	275, 285
AES 128	CBC	Encryption of media	128	173, 183
AES 256 (FIPS 197)	CBC	Encryption of media Encryption of media keys Encryption of pool keys Encryption of catalogs	256	173,183

- Asymmetric Key Algorithms

Algorithm	Modes Implemented	Use	Key Sizes	Certificate #
RSA (FIPS 186-2)	PKCS #1 V1.5	Electronic sign & verify operations	1024	26

- Hashing Algorithms

Algorithm	Use	Certificate #
SHA-1	Hash digest for signing log files.	269,258
SHA-512	Not Used at this time.	269

- HMAC

Algorithm	Use	Certificate #
HMAC-SHA-1	Hash digest for configuration files. Hash digest for tape blocks	25
HMAC-SHA-512	Hash digest for configuration files. Hash digest for catalogs Hash digest for Tape Header	25

- Random number generator

Specification	Use	Certificate #
ANSI 9.31	Key generation	35

The following table describes the keys stored or used by the module.

CSP Description	Use	Key Type	Generation	Storage
Key Encrypting Key (KEK)	Used to encrypt other keys	AES 256	Generated automatically using PRNG compliant to ANSI X9.31 or electronically recovered.	Stored in secured NVRAM
Message Authentication Code Key (HMAC)	To protect configuration files	HMAC	Generated automatically using PRNG compliant to ANSI X9.31 or electronically recovered.	Stored in secured NVRAM

CSP Description	Use	Key Type	Generation	Storage
Pool Encryption Key (PEK)	Used to encrypt TEK/HMAC	AES 256	Generated automatically using PRNG compliant to ANSI X9.31 or electronically recovered.	Stored on hard disk encrypted by KEK
Pool MAC Keys (HMAC)	Used to authenticate Tape Header Block using HMAC-SHA-512	HMAC-SHA-512	Generated automatically using PRNG compliant to ANSI X9.31 or electronically recovered.	Stored on hard disk encrypted by KEK
Tape Encryption Keys (TEK)	Used to encrypt user data	AES 128 AES 256 TDES	Generated automatically using PRNG compliant to ANSI X9.31.	Stored on hard disk or tape media encrypted by either KEK or PEK
Tape MAC Keys (HMAC)	Used to authenticate user data using HMAC-SHA-1	HMAC-SHA-1	Generated automatically using PRNG compliant to ANSI X9.31.	Stored on hard disk or tape media encrypted by either KEK or PEK
Remote Access	SSL/SSH remote access	RSA	Generated automatically using PRNG compliant to ANSI X9.31.	Private key portion stored in secured NVRAM
RNG Key	Key used as constant as part of the ANSI RNG	TDES	Static key	Stored in the firmware
2-factor Authentication Key	Additional authentication method for user access to module	TDES	16 bits generated automatically using PRNG compliant to ANSI X9.31 with 1st 8 bits appended to the end to produce 24 bits.	Stored encrypted using the APK onto the hard disk.

CSP Description	Use	Key Type	Generation	Storage
Authentication protection key (APK)	Encrypts password files and RSA private keys stored in module	TDES	Generated automatically using PRNG compliant to ANSI X9.31.	Stored in secured NVRAM
Software/firmware load key	Verification of integrity of firmware	RSA	Key pair generated at Neoscale with public key stored on the module	Public key stored on the module
Passwords	Authentication	NA	Created by the Administrator	Stored encrypted using the APK onto the hard disk.

Key Input & Output

Keys may be electronically entered or exported (archived) in encrypted form. Archiving of the keys can only be done using split-key (M of N) export when in FIPS compliant mode. Keys cannot be exported from the CryptoStor Tape 700 Series in cleartext form.

Key Generation

Keys are generated automatically using the PRNG complaint to ANSI 9.31.

Key Storage & Destruction

The system keys (KEK and HMAC) are stored in cleartext in secured NVRAM and are not accessible to anyone without tampering the unit causing zeroization of the secured NVRAM. The pool keys are stored in encrypted form using the system keys. The tape keys are stored in encrypted form using the system keys or pool keys.

Manual Key Zeroization

A Security Officer can manually zeroize system keys by issuing the "***zeroize***" CLI command or by issuing the "***Destroy Keys***" command from the Web UI.

Self-tests

The CryptoStor Tape 700 Series performs the following self-tests at power up. These self tests are run without any operator intervention during each occurrence of the unit being powered up.

- RNG KAT
- Cryptographic algorithm KAT for all implementations of AES, TDES, RSA, HMAC-SHA-1 (includes test for SHA-1) and HMAC-SHA-512 (includes test for SHA-512)
- Cryptographic algorithm KAT for SHA-1 hardware implementation
- Software/firmware integrity test
- DDR memory test
- NVRAM test
- Flash memory test
- Box open status test
- Bypass test

Data ports are offline until satisfactory completion of power-up self-tests.

The failure of any self-test will result in the module transitioning into the error state. When an error is encountered, the module will return an error status message pertaining to the error encountered via the CLI. The operator can attempt to clear the error by rebooting the module. Failing this, the module must be sent to Neoscale for Service.

Conditional tests

The CryptoStor Tape 700 Series performs the following conditional tests.

- Continuous RNG test
- Pair-wise consistency test
- Firmware load test

EMC/EMI

The CryptoStor Tape 700 Series is independently tested and complies with code 47 of FCC regulations, Part 15, Subpart B for class B equipment.

Design Assurance

Configuration management is established with the use the Concurrent Versions System (CVS). This version control system is the primary configuration management system used for the CryptoStor line of products. It is provides all standard version control features needed to maintain a history of a source tree – be it software, FPGA, board design or documentation.
All configuration items (parts, documents, software, user guidance) of the module are assigned with a unique identification number and labeled accordingly.

Approved FIPS Mode of Operation

When operating the CryptoStor Tape 700 Series in the FIPS mode of operation, the following rules are enforced:

- Exporting or importing of System Keys (KEK and HMAC) must be done using split-key (M, N) export.
- The Configuration File is exported separate from the System Keys.
- The Catalog is exported encrypted by the System Key only. The System Key is exported separately using a smart card.

The CryptoStor includes the following non-approved security functions when not set to the FIPS mode of operation:

- Exporting of System Keys to a file or smartcard in encrypted form using a passphrase.
- Importing of System Keys in encrypted form using a passphrase.
- Exporting of the Configuration File along with System Keys onto a smartcard.
- Exporting/Importing the Catalog using a passphrase.

Set Up and Initialization Procedure for the FIPS Mode of Operation

To setup the CryptoStor Tape 700 Series in the FIPS mode of operation, perform the following instructions:

- After the initial boot process, log in as administrator using the default password.
- Change the Administrator default password as instructed.
- Create a Security officer account.
- Enter the hostname and configuration parameters for the CryptoStor.
- Generate RSA (SSL) Certificate
- Login to the Tape 700 Series as Security Officer through the CLI.
- Change password.
- Inject System Keys
- Enter the command *set fipsmode on*

To verify the FIPS mode of operation is set:

- Login to the Tape 700 Series GUI management console as either the Administrator or Crypto Officer
- Select the System: Summary page.
- Verify FIPS Mode of Operation is set to yes.
- Set up a Security Policy
- Restart the device.