CryptoStor Tape 700 Family
Security Policy
Non-Proprietary

NeoScale Systems, Inc.

November 12th, 2008

Document Revision: 13

TABLE OF CONTENTS

Document History

Rev	Comments	Author	Date
0.1	Initial draft	H. Puri	12/31/2004
0.2	Changed name to 700 Family	H. Puri	02/18/2005
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	R. Quijano-Nguyen	11/16/2005
0.8	Additional requirements from NIST/CSE	R. Quijano-Nguyen	01/09/2006
0.9	Updated and included FC702R and FC704R Models	R. Quijano-Nguyen	10/6/2006
0.10	Included SC702R & updated the document based on internal analysis	R. Quijano-Nguyen	1/3/2007
0.11	Reflected functional testing inputs/results and algorithm certificate numbers	R. Quijano-Nguyen	3/2/2007
0.12	Modified based on feedbacks from CMVP	J. Huang	7/31/2008
0.13	Changed two cases of “certified” to “validated” Modified, based on feedbacks from CMVP	J. Huang	11/12/2008

Introduction

Purpose

This is a non-proprietary Cryptographic Module Security policy for the CryptoStor Tape 700 Family from NeoScale Systems, Inc. This security policy describes how the CryptoStor Tape 700 Family of security appliances meets the security requirements of FIPS 140-2 and how to run one of these appliances in an approved mode of operation. This document was prepared as part of the Level 3 FIPS 140-2 validation of the Tape 700 Family. CryptoStor Tape family members support either Fibre Channel (FC) or SCSI interfaces giving unparalleled flexibility. NeoScale's Tape 700 Family consists of the following models:

- CryptoStor Tape FC702 and FC704 are Fibre Channel (FC). These models are FIPS validated under certificate number 621.

  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

- CryptoStor Tape FC702R, FC704R, and SC702R are new models. These three new models were added to the family of validated configurations. These have identical functionality to the previously-validated models. FC702R and FC704R have Fibre Channel interfaces and SC702R has SCSI interface. There were also some cosmetic changes to the user Interface (UI) that are not security relevant.

  FC702R P/N FAS00005-00 Rev 6 FW: 2.6

  FC704R P/N FAS00006-00 Rev 8 FW: 2.6

  SC702R P/N FAS00004-00 Rev 6 FW: 2.6

The RoHS Directive stands for "the restriction of the use of certain hazardous substances in electrical and electronic equipment". This directive restricts the use of new electrical and electronic equipment containing more than agreed levels of lead, cadmium, mercury, hexavalent chromium, polybrominated biphenyl (PBB) and polybrominated diphenyl ether (PBDE) flame retardants. It is closely linked with the Waste Electrical and Electronic Equipment Directive (WEEE) 2002/96/EC which sets collection, recycling and recovery targets for electrical goods and is part of a legislative initiative to solve the problem of huge amounts of toxic e-waste.

References

This document provides information on the security operations and capabilities of the Tape 700 Family as it relates to FIPS 140-2. More information is available on the Tape 700 Family 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 appliances. 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 Family is designed to comply with the overall requirements of FIPS 140-2, level 3. The following table indicates appliance level compliance as applicable:

Security Requirements Section	Level
Cryptographic Appliance Specification	3
Cryptographic Appliance 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 Appliance Security Policy	3
Overall Level of Validation	3

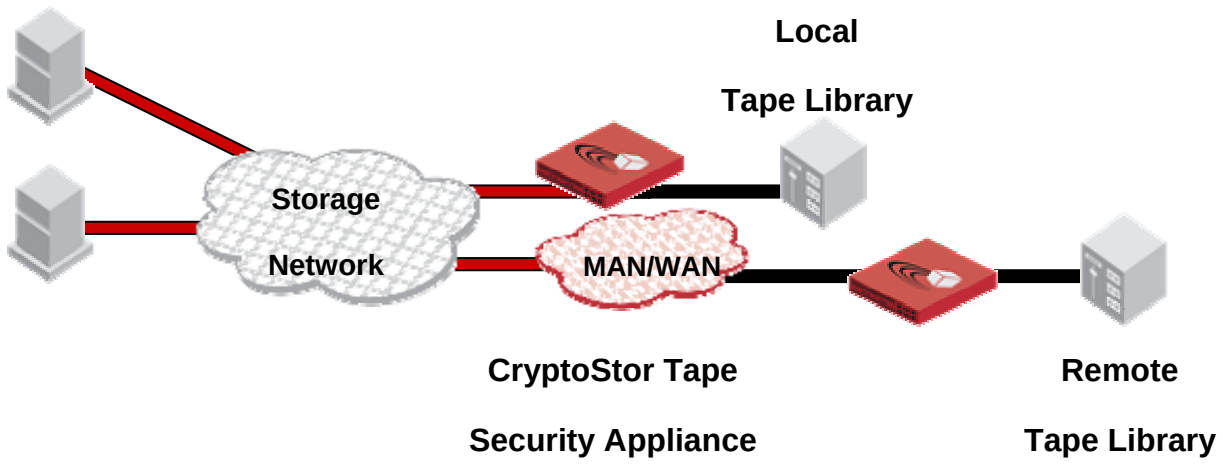
Table 1 FIPS 140-2, Level 3 Requirements

The CryptoStor Tape 700 Family 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/FC704 and FC702R/FC704R appliances, referred in this document as the Tape 700 Family, 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 Family 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 Family is a multi-chip standalone appliance and the cryptographic boundary of the appliance 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 Family Interfaces

The Tape 700 Family provides a number of physical and logical interfaces to the device. The physical interfaces provided by the Tape 700 Family 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
Data Input Interface	SCSI Port
Data Output Interface	SCSI Port
Control Input Interface	10/100/1G BASE-TX LAN Port, Console port
Status Output Interface	2 FC702 Port LEDs, 4 FC702 Port LEDs, 2 SCSI Port LEDs, 2 Power Port LEDS, 10/100/1G BASE-TX LAN port, Console port, Front Panel Display, smart card connector
Power Interface	PCI Compact Power Connector

Table 2 – FIPS 140-2 Fibre Channel & SCSI Logical Interfaces

Currently, the Tape 700 Family consists of four systems:

- The FC702 system has two Fibre Channel ports and two encryption cards.
- The FC704 system has four Fibre Channel ports and four encryption cards.
- The FC702R is identical to the FC702. The only difference is that the FC702R is RoHS compliance.
- The FC704R is also identical to the FC704. The only difference is that the FC704R is RoHS compliance.
- The SC702R is identical with the previously validated models, FC702/FC704. Minor differences are that the SC702R is RoHS compliance as well as it has an SCSI interface rather than a Fibre Channel interface.

Roles and Services

The Tape 700 Family supports identity-based authentication. Users authorized to access the appliance are required to enter a username and password to authenticate their identity to the system in order to perform tasks that are authorized for their type of user (role). Users access the Tape 700 Family by either:

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

Administrators of the appliance choose their own passwords and create the user-IDs for security and recovery officers. The security officers and the recovery officers choose their passwords which they can change at any time.

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 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.

User Account Lockout

For login attempts, the authentication mechanism is designed with an account-locking feature where three consecutive login failures for a given user ID will lockout access for that user. The account will be unlocked only when a user with an administrator or security officer role unlocks it. Security officers can unlock other security officers or recovery officers, but they cannot unlock administrators. The locking feature does not apply to administrator privileged login failures through the console. Hostile attack through the console is not considered likely because physical access to the appliance is required.

When an administrator account is locked, the administrator must login via the console and change their own password, or another administrator must reset their password. When a security officer account is locked, the officer must login via the serial console and change their own password, or another security officer must reset their password.

On the serial console, the system imposes a minimum of a 1-second delay for each login attempt. After four unsuccessful login attempts, the serial console disconnects. Assume a worst-case scenario that an attacker attempts to guess a password on the serial console. Further, assume that the attacker is able to reconnect immediately to the console after a serial port disconnect. Such an attacker would be able to guess passwords at a rate of one guess per second.

On average, a well-chosen 8-character password would require an attacker to try half of the possible password permutations (**361102068154368** password attempts). At a rate of one guess per second, an attacker would require an average of over **11442869** years (361102068154368 / (60 * 60 * 24 * 365.2425).

The appliance 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 Family 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 Family 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 Family CLI or GUI after providing proper user ID and corresponding password.

Role	User	***Type of Authentication***	***Authentication Data***
*Super User	User	Identity-based	The operator is granted access to the Tape 700 Family CLI or GUI after providing proper user ID and corresponding password.

Table 3 – Tape 700 Family Roles

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 Family such as:

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

Security Officer Role

The Security Officer is responsible the security related aspects of the Tape 700 Family such as:

- System key management
- Implementation and management of security policies
- 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 Family 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 tape label	Configuration file	W
	Import/export catalogs	Key Encrypting Key (KEK)	E
	Create/modify/delete security policies	Configuration file	W
	View system & audit log	None	R
	Export system & audit log files	Key Encrypting Key (KEK)	E
	Inject system keys	Encryption Key	E
	Change own password	Password	W
	View/import certificates	None	R, W
Recovery Officer	Recover 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.		

Table 4 – Tape 700 Family Services

Security Functions

Security functions consist of:

- Physical security
- Cryptographic key management
- Key input & output
- Key generation
- Key storage & destruction
- Manual key zeroization
- Self-tests
- Conditional tests

Physical Security

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

The cryptographic security boundary is defined by the opaque sheet metal enclosure of the appliance 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 appliance 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 Family 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 appliance 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 appliance. 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 Family is provided by 4 fans mounted external to the front of the main sheet metal enclosure. These fans blow air into the appliance 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 illustrate where to place tamper seal evidence. One tamper seal is placed in middle left corner and the other tamper seal is placed in 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 as shown on the following pictures.

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 & 516
AES 128, 256 (FIPS 197)	CBC	Encryption of media	128, 256	173 & 506

Table 5 – Symmetric Key Algorithms

- Asymmetric Key Algorithms

Algorithm	Modes Implemented	Use	Key Sizes	Certificate #
RSA (FIPS 186-2)	PKCS #1 V1.5	Electronic sign & verify operations	1024	221

Table 6 – Asymmetric Key Algorithms

- Hashing Algorithms

Algorithm	Use	Certificate #
SHA-1	Hash digest for signing log files	258 & 577
SHA-512	Use to produce HMAC-SHA-512 values	258 & 577

Table 7 – Hashing Algorithms

- HMAC

Algorithm	Use	Certificate #
HMAC-SHA-1	Hash digest for configuration files Hash digest for tape blocks	39 & 259
HMAC-SHA-512	Hash digest for configuration files Hash digest for catalogs Hash digest for Tape Header	39 & 259

Table 8 – HMAC

- Random number generator

Specification	Use	Certificate #
ANSI X9.31	Key generation	285

Table 9 – RNG

- Keys stored or used by the appliance

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

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
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

CSP Description	Use	Key Type	Generation	Storage
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	TDES	Static key	Stored in the firmware
2-factor Authentication Key	Additional authentication method for user access to appliance	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.
Authentication protection key (APK)	Encrypts password files and RSA private keys stored in appliance	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 appliance	Public key stored on the appliance
Passwords	Authentication	NA	Created by the Administrator	Stored encrypted using the APK onto the hard disk.

Table 10 – Tape 700 Family Keys Storage

Key Input & Output

Keys may be electronically entered or exported (archived) in encrypted form. Keys cannot be exported from the CryptoStor Tape 700 Family in cleartext form.

System Key

Archiving of the keys can only be done using split-key (M of N) export to or import from smart card when in FIPS compliant mode.

Tape Keys and Pool Keys

Keys may be electronically entered or exported (archived) in encrypted form via file.

Key Generation

Keys can be build manually or 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 appliance 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 the system key by issuing the "***zeroize***" CLI command or by issuing the "***Destroy Keys***" command from the Web UI.

Self-tests

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

- RNG Known Answer Test (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).
- Firmware integrity test (CRC 32).
- Yargon memory test.
- Non-Volatile Random Access Memory (NVRAM) test.
- Box open status test.

The data flow on the Fibre or SCSI channel ports is inhibited while self-test are running and when module enters into the error state.

The console will indicate if the power-up self test have completed successfully and the LCD display says “ready”. The power-up self test can be executed by cycling the appliances’ power. The failure of any self-test will result in the appliance transitioning into the error state. If the display shows an error condition, check all cabling and power cycle the appliance by removing both power cords and reinserting them. If the appliance still shows an error, contact NeoScale Customer Support.

Conditional tests

The CryptoStor Tape 700 Family performs the following conditional tests.

- Bypass mode test
- Continuous RNG test
- RSA Pair-wise consistency test
- Software install test
- Firmware load test

EMI/EMC

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

Design Assurance

NeoScale uses two version controls systems. Agile is used to manage communications and information with NeoScale’s suppliers (SCM-Supply Chain Management). Bill of Materials (BOMs) user documentations, drawings, and schematics are tracked in Agile.

NeoScale also uses Concurrent Versions System (CVS) for tracking software builds and changes while it is in development and testing stage. Once a software build is ready for external use, it gets release into to Agile for production.

Approved FIPS Mode of Operation

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

- Exporting or importing of System Key (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 Key to a file or smart card in encrypted form using a passphrase.
- Importing of System Key in encrypted form using a passphrase.
- Exporting of the Configuration File along with System Key onto a smart card.
- Exporting/Importing the Catalog using a passphrase.

Setting the Appliance to Operate in FIPS Mode

To set the CryptoStor Tape 700 Family to operate in FIPS mode:

1. Log in as an Administrator using the default password `password`.
2. Change the default Administrator password when prompted.
3. Run the interactive CLI command `setup` and enter the network configuration information.
4. Use the GUI to create a Security Officer account and note the temporary password.
5. Log in as a Security Officer and change the temporary password.
6. Use the GUI to inject the system keys.
7. Log in as a Security Officer and run the `set fipsmode on` CLI command. The appliance is now running in FIPS mode.

To verify the appliance is running in FIPS mode:

1. Log in to the appliance GUI management console as either the Administrator Security Officer.
2. Select the System: Summary page.
3. Verify that FIPS Mode of Operation is set to `Yes`.

Distribution and Delivery

NeoScale appliances have a tampered seals applied on the top cover after final inspection and prior to packaging the appliance. This will insure that that all NeoScale appliances reach the end user secured and allows detection of unauthorized modifications of the appliance. In addition, NeoScale uses a bonded courier for delivery. The user documentations also describe the steps to be used for the secure installation, generation, and start-up of the appliance.

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
EMI/EMC	Electromagnetic interference/electromagnetic compatibility
FIPS	Federal Information Processing Standard
FW	Firmware
GUI	Graphical User Interface
HMAC	Keyed-Hash Message Authentication Code
KAT	Known Answer Test
LUN	Logical Unit Number
NIST	National Institute of Standards and Technology
PKCS	Public Key Cryptography Standards
RNG	Random Number Generator
RSA	RSA is an algorithm for public-key encryption
SAN	Storage Area Network
SHA	Secure Hasing Algorithm
SSL	Secure Sockets Layer
SSH	Secure Shell
UI	User Interface