CryptoStor FC2002W

P/N: 820-0001-06 Rev2
FW: Rev 2.2.2

Non-Proprietary Security Policy
Revision 0.10

NeoScale Systems, Inc.
October 20, 2005

TABLE OF CONTENTS

Document History

Revision	Comments	Author	Date
0.1	Initial draft	M. Liedstrand	6/30/04
0.2	Updates after initial review with Domus Labs	M. Liedstrand	8/10/04
0.3	First version submitted to Domus Labs	M. Liedstrand	10/1/04
0.4	Added Certificate numbers.	Dharmesh Shah	3/31/2005
0.5	Incorporated Domus comments for NIST	Rose Quijano-Nguyen/Samiullah Mohammed/Bob Lockhart	7/22/2005
0.6	Network User Updated	Rose Quijano-Nguyen	7/25/05
0.7	Additional Changes from Domus	Rose Quijano-Nguyen	7/25/05
0.8	Removed Network User	Rose Quijano-Nguyen	9/28/05
0.9	Updated based on 10/14 feedback from CSE & NIST (through Domus)	Rose Quijano-Nguyen	10/18/05
0.10	Changed Security Officer Roles	Rose Quijano-Nguyen	10/20/2005

Acronyms and Abbreviations

AES	Advanced Encryption Standard
CM	Cryptographic Module
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
DES	Data Encryption Standard
FIPS	Federal Information Processing Standard
NIST	National Institute of Standards and Technology
RNG	Random Number Generator

Introduction

Purpose

This is a non-proprietary Cryptographic Module Security policy for the CryptoStor FC2002W from NeoScale Systems, Inc. This security policy describes how the FC2002W SAN Security Appliance meets 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 FC2002W.

References

This document provides information on the security operations and capabilities of the FC2002W as it relates to FIPS 140-2. More information is available on the FC2002W 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 FC2002W 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 FC2002W 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 FC2002W appliance, referred to in this document as the FC2002W, is a Fibre Channel Storage Area Network (SAN) data security appliance that provides data flow control and encryption based on configured policy rules. Operating as a fully transparent, in-line storage appliance, the FC2002W inspects storage traffic and applies information flow controls and strong encryption to the data payload at gigabit rates. Storage data privacy policies are centrally managed, employing access and encryption rules which are easily modified to suit current and evolving storage infrastructures. Deep frame inspection allows access and encryption policies to be dynamically applied at wire-speed. True gigabit throughput with low latency and transparent operation ensures uninterrupted, scalable storage data protection.

The FC002 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.

FC2002W Interfaces

The FC2002W provides a number of physical and logical interfaces to the device. The physical interfaces provided by the FC2002W 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; Smartcard connector
Control Input Interface	Smart Card 10/100BASE-TX LAN, Port Console, Smart Card used for system key archival.
Status Output Interface	LEDs, 10/100BASE-TX LAN port, Console Port, Front Panel Display
Power Interface	PCI Compact Power Connector

Table 1 – FIPS 140-2 Logical Interfaces

Roles and Services

The FC2002W 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 FC2002W 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.

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 FC2002W CLI or GUI after providing proper user ID and corresponding password.
Security Officer	Crypto-Officer	Identity-based	The operator is granted access to the FC2002W CLI or GUI after providing proper user ID and corresponding password.
Recovery Officer	Crypto-Officer	Identity-based	The operator is granted access to the FC2002W CLI or GUI after providing proper user ID and corresponding password.

Each of these roles is described and discussed below.

Administrator Role

The Administrator is responsible for configuring the non-security services of the FC2002W.

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 FC2002W such as the implementation and management of security policies and system key management.

Typical functions allowed to an Security Officer are:

- Security Office 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
- Encryption/Decryption

Recovery Officer Role

The Recovery Officer is responsible for archiving and recovery of the system keys.

Services

The FC2002W 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
	Enable/disable ports	None	E
	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	Create/modify/delete Security Officer account	None	R, W
	Create/delete system keys	Key Encrypting Key (KEK)	W, E
	Encryption/Decryption	Encryption Key	E
	Create recovery system key shares	Key Encrypting Key (KEK)	W, E
	Create/delete/view encryption keys	Encryption key	W, E
	Zeroize keys	None	E
	Create/modify/delete security policies	HMAC	W
	View system & audit log	None	R
	Export system & audit log files	Key Encrypting Key (KEK)	E
	View/import certificates	None	R, W
Recovery Officer	Export/import recovery system key share	Key Encrypting Key (KEK)	R, W

Role	Authorized Services	Cryptographic Keys and CSPs	Type(s) of Access

Security Functions

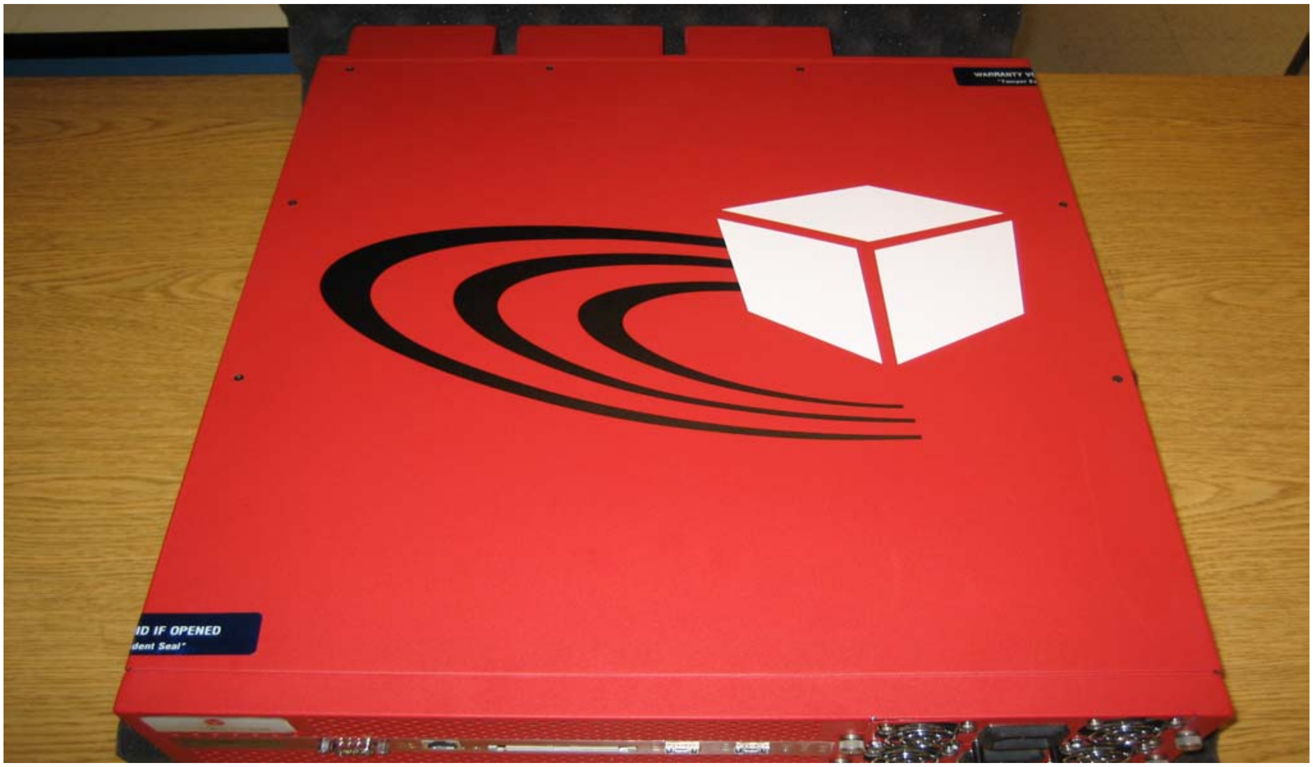
Physical Security

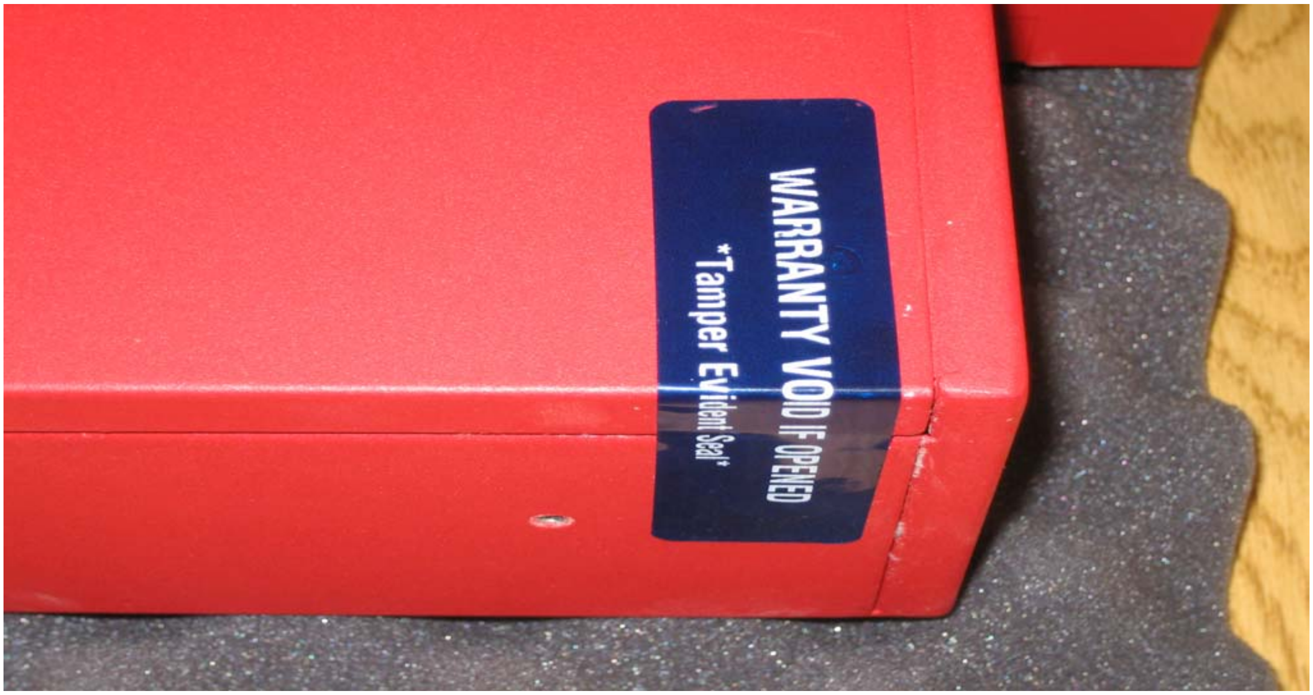
The CryptoStor FC2002W is a multi-chip standalone cryptographic module designed to meet FIPS 140-2, level 3 for physical security. The module consists of production grade components with standard passivation techniques applied.

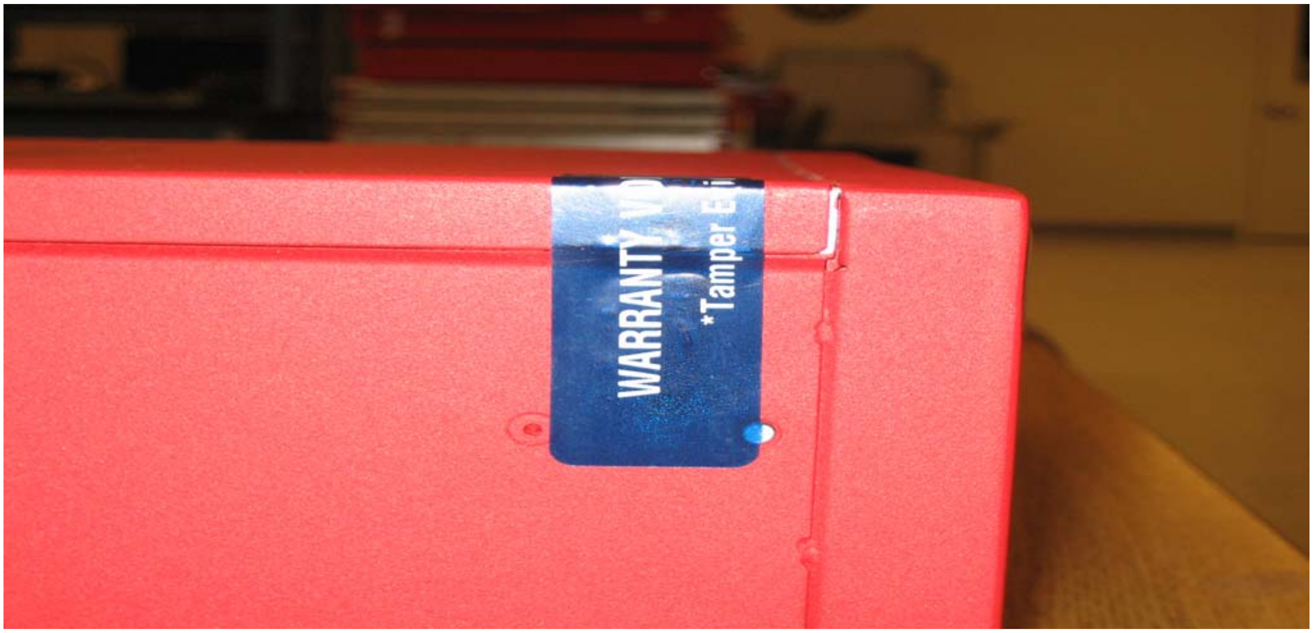
The cryptographic security boundary is defined by the unit's opaque sheetmetal enclosure with the exception of the fan and power supply modules which are field replaceable. Access to the circuitry is restricted through the use of tamper-evidence labels applied to the removable cover and the chassis showing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

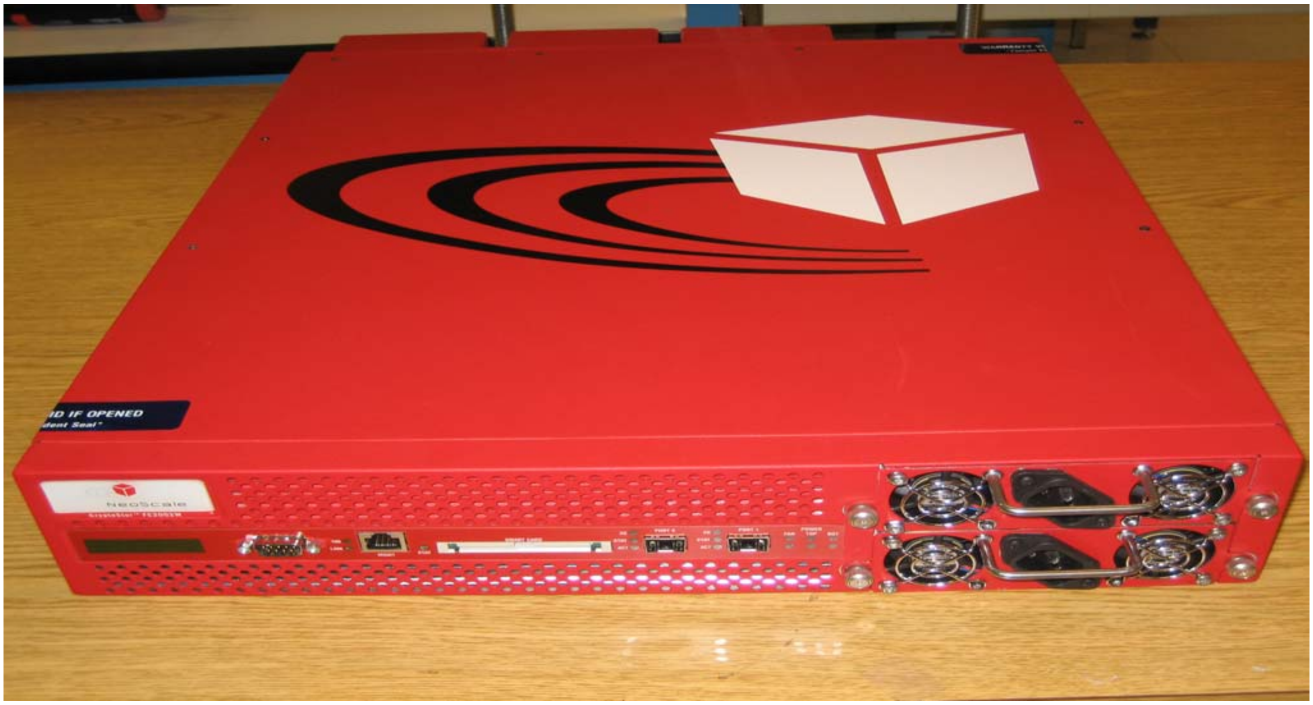
The FC2002W is 2U (3.75 inches) high by 17.3 inches wide by 22.25 inches deep. It includes a single access cover protected with tamper-evident labels and the tamper response and zeroization circuitry. The unit contains 2 printed circuit board assemblies connected through a micro high-speed interface connector/socket combination. The smaller PCB containing the cryptographic functions is roughly 11 x 8 inches. The larger PCB containing processor, controller and data path functions is roughly 11 x 17 inches. The 2 redundant power supplies are externally accessible from the front of the module. The power is brought to the PCBs through a power interface connector, mounted at the rear of the power supply cavity containing the power supplies, and a harness connecting directly to the PCBs. Cooling for the FC2002W is provided by 3 fans mounted external to the main sheet metal enclosure which blows are 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 lower left corner of FC2002W and the other tamper seal is placed upper right corner. Each tamper seals sit on top or cover a screw. The only way to get to the cover is to break the tamper seals.


WARRANTY VO
*Tamper Ev
ID IF OPENED
dent Seal*


WARRANTY VOID IF OPENED
Tamper Evident Seal


WARRANTY VO
*Tamper E


RD IF OPENED
dent Seal*
NeoScale

Secured NVRAM

Tamper response and zeroization circuitry destroys plaintext CSPs stored in the secured NVRAM upon removal of the cover.

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 (FIPS 197)	CBC	Encryption of media; Encryption of media keys	256	173, 183

- Assymmetric 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

- HMAC

Algorithm	Use	Certificate #
SHA-1	Hash digests for configuration file.	25
SHA-512	Hash digests for configuration file.	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.

Key Description	**Use**	**Key Type**	**Generation**	**Storage**
Key Encrypting Key (KEK)	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
Media Keys	User to store user data	AES 256 TDES	Generated automatically using PRNG compliant to ANSI X9.31.	Stored in secured NVRAM
Remote Access	SSL/SSH remote access	RSA	Generated automatically using PRNG compliant to ANSI X9.31.	Private key portion stored in secured NVRAM
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 PPK onto the hard disk.
Password protection key (PPK)	Encrypt password file 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	

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 FC2002W 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 media keys are stored in encrypted form using the system keys.

Zeroize Command

“Zeroize” is a Command Line Interface (CLI) command used for key zeroization without tripping the tamper switches. Opening the cover results in tripping the tamper switches.

Self-tests

The CryptoStor FC2002W 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 and SHA-1.
- Software/firmware integrity test
- FPGA programming test
- DDR memory test
- d test
- Flash memory test
- Box open status test
- Configuration Policy File Integrity 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 FC2002W performs the following conditional tests.

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

EMC/EMI

The CryptoStor FC2002W 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 FC2002W in the FIPS mode of operation, the following rules are enforced:

- Exporting or importing of System Keys must be done using split-key (M, N) export.
- The Configuration File is exported separate from the System Keys.

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.

Set Up and Initialization Procedure for the FIPS Mode of Operation

To setup the CryptoStor FC2002W in the FIPS mode of operation, perform the following instructions:

- After the initial boot process, log in an administrator using the default password.
- Change the Administrator default password as instructed.
- Enter the hostname and configuration parameters for the CryptoStor.
- Log in as the Security Officer using the default password.
- Change the Security Officer default password as instructed.
- Login to the FC2002W as Security Officer through the CLI.
- Enter the command *set fipsmode on*

To verify the FIPS mode of operation is set:

- Login to the FC2002W GUI management console as either the Administrator or Crypto Officer
- Select the System: Summary page.
- Verify FIPS Mode of Operation is set to yes.