



**NitroView Receiver
Version 8.0.0.20080605
Security Policy**

FIPS 140-2 Level 2 Validation



Model Numbers
NS-RCV-2250-R

March 13, 2009
Version 1.12

1	Introduction	3
1.1	Acronyms and Abbreviations	4
2	NitroSecurity NitroView Receiver	6
2.1	Functional Overview	6
2.2	Module Description	7
2.3	Module Ports and Interfaces	7
3	Security Functions	9
4	FIPS Approved Mode of Operation	10
4.1	Set-Up and Initialization Procedures.....	10
5	Identification and Authentication	11
6	Cryptographic Keys and CSPs	12
7	Roles and Services	14
8	Access Control	14
9	Physical Security	16
10	Self Tests	17
11	Mitigation of Attacks	18
12	References	18

1 Introduction

This document is the Security Policy for NitroSecurity NitroView Receiver cryptographic module. This Security Policy specifies the security rules under which this cryptographic module shall operate to meet the requirements of FIPS 140-2 Level 2. It describes how the module functions to meet the FIPS requirements, and the actions that operators must take to maintain the security of the module.

This Security Policy describes the features and design of the NitroView Receiver cryptographic module using the terminology contained in the FIPS 140-2 specification. *FIPS 140-2, Security Requirements for Cryptographic Modules* specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information. The NIST Cryptographic Module Validation Program (CMVP) validates cryptographic modules to the FIPS 140-2 standard. The Cryptographic Algorithm Validation Program (CAVP) validates algorithms used by a FIPS validated module. Validated products are accepted by the Federal agencies of both the USA and Canada for the protection of sensitive or designated information.

The FIPS 140-2 standard and information on the CMVP can be found at <http://csrc.nist.gov/groups/STM/cmvp>. Information on the CAVP can be found at <http://csrc.nist.gov/groups/STM/cavp>. More information describing the NitroView ESM can be found at <http://www.NitroSecurity.com>.

In this document, the NitroSecurity NitroView Receiver is also referred to as “the Receiver”, or “the module”.

This Security Policy contains only non-proprietary information. All other documentation submitted for FIPS 140-2 conformance testing and validation is “NitroSecurity - Proprietary” and is releasable only under appropriate non-disclosure agreements.

The NitroSecurity NitroView Receiver cryptographic module meets the overall requirements applicable to Level 2 security for FIPS 140-2 as shown in Table 1.

Table 1. Cryptographic Module Security Requirements.

<i>Security Requirements Section</i>	<i>Level</i>
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles and Services and Authentication	2
Finite State Machine Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A
Cryptographic Module Security Policy	2

Document Version History

Version	Date	Comments	Name
1.00	5/15/08	Initial Draft	Ward Rosenberry
1.01	6/11/2008	2 nd internal draft	Ward Rosenberry
1.02	7/11/08	3 rd internal draft	Ward Rosenberry
1.03	8/1/08	Submission draft	Ward Rosenberry
1.04, 1.05	8/20/08, 10/16/08	Incorporate evaluator comments	Ward Rosenberry
1.06	12/23/08	Incorporate evaluator comments from NIST	Bill Virtue
1.08	1/14/09	Incorporate evaluator comments from SAIC	Bill Virtue
1.09	2/11/09	Updated with changes from CSE	Bill Virtue
1.10	3/11/09	Updated with changes from CSE	Bill Virtue
1.11	3/13/09	Updated with changes from CSE	Bill Virtue

Formatted Table

1.1 Acronyms and Abbreviations

AES	Advanced Encryption Standard
CFB	Cipher Feedback
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
CSP	Critical Security Parameter
DRNG	Deterministic Random Number Generator
DH	Diffie-Hellman Algorithm
DSA	Digital Signature Algorithm
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
ECDH	Elliptic Curve Diffie-Hellman
EDC	Error Detection Code
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
HMAC	Keyed-Hash Message Authentication Code
KAT	Known Answer Test
LAN	Local Area Network
LED	Light Emitting Diode
NDRNG	Non-Deterministic Random Number Generator
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
PRNG	Pseudo Random Number Generator
PUB	Publication
RAM	Random Access Memory
ROM	Read Only Memory
RNG	Random Number Generator
RSA	Rivest Shamir Adleman public key cryptosystem
SHA-1	Secure Hash Algorithm
SHA-384	Secure Hash Algorithm

SDEE	Security Device Event Exchange
RDEP	Remote Data Exchange Protocol
NPP	NitroSecurity Plug-In Protocol
T-DES	Triple-DES (Data Encryption Standard)

2 NitroSecurity NitroView Receiver

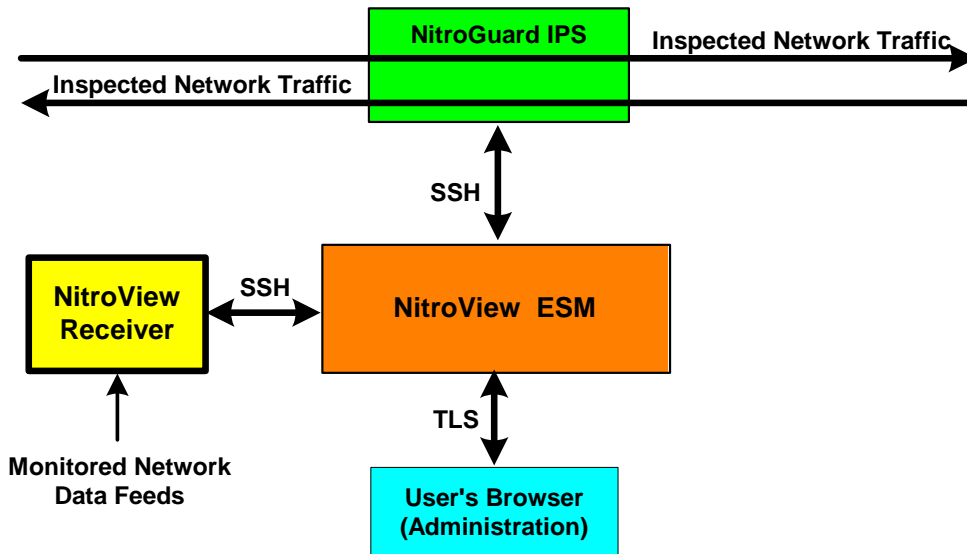
2.1 Functional Overview

NitroSecurity provides highly scalable enterprise security solutions that provide intrusion prevention, network behavior analysis and security event management enabling enterprises to secure their networks with real-time threat mitigation. The NitroView Receiver enables the collection of security events and network flow data from multi-vendor sources including firewalls, IPS/IDS, NetFlow and others. The NitroView Receiver is an integral component of a comprehensive security management solution with the ability to gather and analyze data from 3rd party network and security solutions.

The NitroView Receiver is unique due to a patented ultra-high-performance aggregation and correlation engine that is integrated into each NitroView Receiver. These sophisticated data acquisition and management capabilities give NitroView Receiver the power to manage thousands of events per second. The Receiver can simultaneously collect both events and network flow data. In addition, it can act as a network monitor to produce flow information directly from the Receiver. Finally, the Receiver has an integrated user configurable correlation engine that can detect patterns of events and flows, and produce events based upon these patterns.

Figure 1 shows a high level functional view of the NitroView Receiver. The Receiver interacts with the NitroView Enterprise Security Manager (ESM), which aggregates and correlates event and network flow data collected from multiple sources including the NitroGuard IPS and the NitroView Receiver. The ESM provides the Receiver management interface. Routine management commands are sent over the SSH channel to the Receiver. The Receiver encrypts the administration channel and data channels between the Receiver and NitroView ESM.

Figure 1. Functional View of the NitroView Receiver Cryptographic Module.



2.2 Module Description

The NitroSecurity NitroView Receiver is a multi-chip standalone cryptographic module consisting of production-grade components contained within an opaque hard production-grade enclosure (the outside case is steel). The removable cover is protected by tamper evident security seals in accordance with FIPS 140-2 Level 2. The cryptographic boundary is the metal enclosure of the device. The module has multiple (general purpose) processors for distributing the workload and improving overall processing efficiency. Use of the various processors is controlled by the operating system and not by Receiver code which views these as a single processor. The module does not include any special purpose processors such as cryptographic accelerators. All of the module services implemented by module software are executed by the general purpose processors, and the memory devices that contain the executable code and data.

The module has a limited operational environment and does not have a bypass mode or a maintenance mode.

The NitroView Receiver meets applicable Federal Communication Commission (FCC) Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC) requirements as defined in Subpart B of FCC Part 15, for Class B devices.

The module uses algorithms from OpenSSL that is built, installed, protected and initialized as specified in the *OpenSSL FIPS 140-2 Security Policy* Version 1.1.2, dated January 29, 2008. Appendix B of the OpenSSL Security Policy specifies the complete set of source files of this module. There are no additions, deletions or alterations of this set as used during module build. All source files, including the specified OpenSSL distribution tar file, are verified as specified in Appendix B of the OpenSSL Security Policy. Installation, protection, and initialization must be completed as specified in Appendix C of the OpenSSL Security Policy. That information is provided to consumers of the Receiver cryptographic module. Any deviation from specified verification, protection, installation and initialization procedures will result in a non FIPS 140-2 compliant module.

Once the software is installed there are no modifications allowed to the OpenSSL or OpenSSH software components. NitroSecurity Linux kernel version 2.6.18.5 is unlikely to be modified.

2.3 Module Ports and Interfaces

The cryptographic module has numerous physical ports and four logical FIPS 140-2 interfaces. The physical ports and logical interfaces are described in Table 2.

Where distinct logical interfaces share the same physical port, communication protocols (such as TCP/IP, and 802.3) and the Receiver application rules of operation logically separate and isolate these interfaces from one another.

Table 2. Physical Ports and Logical FIPS 140-2 Interfaces.

<i>Physical Port</i>	<i>Description</i>
Front Panel	
Power On Switch	Power input
Power Off Switch	Power input
Arrow Keys	Control input for the front panel LCD
LCD Display	Status output
Rear Panel	
Management Port 1	Network interface connector for control input, status output, data input and data output. The network interface card is an RJ45 copper interface (10/100/1000 megabit). This port may connect to a managing NitroSecurity Enterprise Security Manager over an SSH tunnel, SDEE/RDEP and NPP data sources, and accepts monitored data feeds directed to the embedded Receiver.

Physical Port	Description
Management Port 2	Network interface connector with the same functionality as Management Port 1. The Receiver may use this as an alternate management port. This port does not support SDEE/RDEP and NPP data sources, and does not accept monitored data feeds directed to the Receiver.
VGA Monitor Port	15-pin D-connector for status output.
Serial Port	Not used.
Mouse Port	PS2 Control input from mouse.
Keyboard Port	PS2 Control input from keyboard.
USB 0	Not used.
USB 1	Not used.
Power Input 1	This is not a FIPS 140-2 logical interface. Power (110 / 220 VAC) enters the module via the power input connectors.
Power Input 1 LED	Green indicates power is available to the module via this power connector. Yellow indicates power is not available at this power connector. Unlit indicates no power is connected to this power connector.
Power Input 2	This is not a FIPS 140-2 logical interface. Power (110 / 220 VAC) enters the module via the power input connectors.
Power Input 2 LED	Green indicates power is available to the module via this power connector. Yellow indicates power is not available at this power connector. Unlit indicates no power is connected to this power connector.
UID Switch	Pressing this switch enables the front LED to identify the unit in a rack of devices. This switch is not available on all Receiver models.

The FIPS 140-2 logical interfaces correspond to physical ports as described in Table 3.

Table 3. FIPS 140-2 Logical Interfaces.

Logical Interface	Description
Data input	Data input consists of: <ul style="list-style-type: none"> plaintext 3rd party security data including events, flows (NetFlow, s-flow, etc.), alerts (firewalls, IPSs, VPNs, etc), host and server log data entering the cryptographic module via Management Port 1 from 3rd party devices on the network for the purpose of being encrypted and forwarded to an ESM. plaintext network traffic enters Management Port 2 and is analyzed to acquire flow data plaintext data sent from SDEE or Nitro Plugin Protocol data sources.
Data output	Data output consists of: <ul style="list-style-type: none"> encrypted 3rd party security data exiting the cryptographic module via Management Port 1 to an ESM over an SSH connection. commands sent to 3rd party devices on the network. The commands are sent via Mgt port 1 to any number of external devices in order to acquire metadata from the devices. Some of the commands sent to external devices are sent in plaintext (e.g. opsec, WMI), and some are sent in FIPS compliant encrypted form (e.g. SDEE and RDEP).

Logical Interface	Description
Control input	Control input consists of: <ul style="list-style-type: none"> • commands from crypto officers entering the module from an ESM in encrypted format via Management Port 1 over an SSH connection. • commands from crypto officers entering the module via the keyboard and mouse ports and the arrow keys on the front of the system
Status output	The status output consists of <ul style="list-style-type: none"> • FIPS operational status returned from status requests by crypto officers. FIPS operational status is output in encrypted format on the SSH connection. The IPS device properties dialog displays the result of the most recent FIPS self-test. • FIPS error status output automatically in plaintext format to the LCD and on HTTP port 4242 (management ports 1 and 2). <p>Module LEDs may also indicate status such as network traffic or the status of power supplied to the module.</p>

3 Security Functions

The NitroView Receiver cryptographic module implements the security functions described in Table 4.

Table 4. Module Security Functions.

Security Function	Purpose or Use	Certificate
Approved Security Functions		
AES (FIPS PUB 197) CBC(e/d; 128)	SSH encryption and decryption.	668
Triple-DES (FIPS PUB 46.3) (CBC)	Support for ANSI X9.31 PRNG	613
SHA-1 (FIPS PUB 180-2) (BYTE-only)	SSH signature generation and verification, data integrity	701
HMAC-SHA1	Data integrity and data authentication within SSH	352 (HMAC), 701 (SHS)
RNG (ANSI X9.31 PRNG, Appendix A.2.4)	Key generation	387
RSA (FIPS PUB 186-2) ALG[RSASSA-PKCS1_V1_5]; SIG(gen); SIG(ver); 2048, SHS: SHA-1 (key transport methodology provides a minimum of 112 bits of encryption strength)	SSH key transport, signature verification	310
Allowed Security Functions		
Diffie Hellman (2048 bit key agreement and key establishment methodology). While not approved, it may be used in FIPS mode.	Key agreement within SSH	Vendor Affirmed

4 FIPS Approved Mode of Operation

The Master Crypto Officer must select FIPS mode during initial configuration. Once in FIPS mode the module performs only FIPS-approved cryptographic algorithms and security functions. When the module is registered with an ESM that is in FIPS mode, the [Receiver] module permanently enters FIPS mode. The module can not register with a NitroView ESM (server) that is not in FIPS mode. The Receiver will only communicate with a FIPS approved mode ESM.

In the FIPS approved mode, crypto officers may configure the module for operation within the IT environment and they may make administrative changes. Users may access the module's data encryption and decryption services by using the Receiver services via an ESM. The FIPS-validated NitroView Receiver allows loading software updates in the field, but this operation must not be used as this operation invalidates the module's FIPS evaluated configuration.

The module supports a non-FIPS mode of operation. If during initial configuration the Master Crypto Officer does not enable FIPS mode, the module will not be in FIPS mode and can only communicate with a non-FIPS mode ESM. Non-FIPS mode communication between the Receiver and ESM exists and is proprietary.

The module supports protocols and functionality that are used within the approved FIPS 140-2 mode of operation and non-approved FIPS 140-2 mode of operation:

FIPS Approved Mode of Operation: OpenSSH (using FIPS-approved cryptographic algorithms and security functions).

Non-FIPS Approved Mode of Operation: SNMP V3, OPSEC (Operations Security), plaintext.

4.1 Set-Up and Initialization Procedures

The NitroSecurity *NitroView Receiver Operator Guidance* provides the following steps to set up and initialize the module into FIPS approved mode:

1. The NitroView ESM (to be used for Receiver management operations) must be configured and operating. The ESM must be a FIPS validated system configured to operate in FIPS approved mode.
2. Check the Receiver packaging and the module, including the two tamper evident seals for signs of tampering. If tampering is detected, contact NitroSecurity Support for further instructions. Place the third tamper-evident seal so it covers the USB ports and the fourth seal so it covers the serial port. These seals can be found in the package of accessories included in the shipping container.
3. Power up the module. While the module boots up, confirm the NitroSecurity software version displayed on the LCD is 8.0.0.20080605. If the version number is different, the module is not the FIPS validated version. Contact NitroSecurity Support for further instructions.
4. After the module boots up, configure the network interface by following the instructions in the *NitroSecurity Installation and Setup Guide* section "Configuring the Network Interface on the Receiver".
5. Complete the setup by using the ESM to add the device to the ESM and register the device to operate with the ESM. Follow the instructions in the *NitroSecurity Installation and Setup Guide* section "Keying the Device".
6. To verify FIPS mode use the NitroView ESM GUI. The bottom 'status' bar indicates that the module is in FIPS mode (shows version / date and "FIPS Enabled"). Using the GUI, select a single device go to device properties, click the FIPS button – runs the FIPS self test and outputs the FIPS status
 - a. Additionally, the master crypto officer is able to see the FIPS status when they authenticate to cryptographic module's console. The FIPS status can be observed when the crypto officer selects the command line option number 3 to determine whether the cryptographic module is in a FIPS approved mode of operation.

5 Identification and Authentication

The module supports two crypto officer roles and a user role. See section [7](#) for more information about these roles.

Multiple concurrent role-based sessions (crypto officer) are allowed. The module's "system administrator", always has the master crypto officer role, and is the only user that can initialize the device using the front panel keys or zeroize the device using the console port on the module. Crypto officers access the module over the SSH channel. Users consist of 3rd party devices that send plaintext or encrypted security data to the module. User data includes events, flows (NetFlow, sFlow, etc.), alerts (from firewalls, IPSs, VPNs, etc), host and server log data, and data from SDEE/RDEP and NPP data sources. The receiver encrypts and forwards user data as needed to an ESM as well as storing data for analysis.

Separation of crypto officer roles is achieved by first requiring authentication before granting access to services offered to a particular authenticated role. The software then programmatically separates roles and services during module use by providing role-specific services to the specific authenticated role. The software programmatically separates concurrent sessions within a role through the use of atomic operations for all operations that change configuration data. The event logging system on the controlling ESM records all access to the system and associates all configuration changes with the identity of the session making the change. Separation of unauthenticated (user) roles is maintained by relying on the protocols and related port assignments to handle user data appropriately.

The module does not display any authentication data entered into the console. Access to the authorized roles is restricted as explained in Table 5:

Table 5. Roles and Required Identification and Authentication.

<i>Role</i>	<i>Type of Authentication</i>	<i>Authentication Data</i>
Master Crypto Officer	Identity-based	Master Crypto Officer Role-based A master crypto officer authenticates by entering a username and a password at the console. Start-up and other operations using the LCD and front panel arrow controls are unauthenticated.
Crypto Officer	Role-based	A crypto officer authenticates by establishing a valid SSH connection with the receiver.
User	None	Users are unauthenticated.

The strength of the operator authentication, per the above roles, is as follows in Table 6:

Table 6. Strength of Authentication.

<i>Authentication Mechanism</i>	<i>Strength of Mechanism</i>
Password	The master crypto officer authenticates using a minimum 8 ASCII-character (Decimal values between 33 and 126, inclusive) password that must include all of the following: one upper case character (A-Z), one digit (0-9), and one special character (printable characters excluding space and alphanumerics, 32 choices). This yields a minimum of 61.1E+12, over 61 trillion, possible combinations; thus, the possibility of correctly guessing a password is less than 1 in 1,000,000. This password is set using the management interface on the management ESM. The possibility of randomly guessing a password in 60 seconds is less than 1

<i>Authentication Mechanism</i>	<i>Strength of Mechanism</i>
	in 100,000. The system allows no more than 6,000 login attempts per minute. Combine this fact with a one in 61 trillion possibility of guessing a password to compute only a 1 in 10.2E+9, over 10 billion, possibility of guessing a password in one minute.
Public key authentication	<p>The Receiver supports public key based authentication with RSA 2048-bit keys. A 2048-bit RSA key has at least 112-bits of equivalent strength. The probability of a successful random attempt is $1/2^{112}$, which is less than 1/1,000,000.</p> <p>The possibility of randomly guessing a key in 60 seconds is less than 1 in 100,000. The system allows no more than 6,000 login attempts per minute. Combine this fact with a one in 61 trillion possibility of guessing a password to compute only a 1 in 10.2E+9, over 10 billion, possibility of guessing a password in one minute.</p>

When the cryptographic module is powered off and subsequently powered on, the results of previous authentications (the authentication states of sessions) are cleared from memory. When the module is powered up again, operators must re-authenticate, entering the correct user name and password.

6 Cryptographic Keys and CSPs

The following table identifies the Cryptographic Keys and Critical Security Parameters (CSPs) used within the module. Cryptographic keys and CSPs are never output from the module in plaintext. An Approved key generation method is used to generate keys that are generated on the module.

Table 7. Cryptographic Keys and CSPs.

<i>Data Item</i>	<i>Description</i>
Receiver SSH Private Key	This RSA 2048-bit private key corresponds to the Receiver SSH Public Key described below in Other Cryptographic Keys. This private key is used for the transfer of key material in the SSH protocol. This key is generated by the FIPS validated RNG (certificate #387) during manufacturing and can never be regenerated again. This key is stored in unencrypted format on an unencrypted disk partition. This key is zeroized according to DoD 5220.22-M when returning the module to the manufacturer for repair or replacement.
SSH AES Encryption Keys	AES 128-bit ephemeral symmetric key used for encrypting and decrypting SSH sessions with ESM devices. This key is produced using DH key agreement. The key is deleted from memory after use.
Diffie-Hellman Keys	Ephemeral Diffie-Hellman public and private parameters used for key agreement to provide SSH AES Encryption Keys. These key parameters are deleted from memory after use.
HMAC Key	The ephemeral HMAC key is used within the SSH protocol for data authentication purposes. It is generated as specified in the SSH protocol specification ¹ (using OpenSSH). This key is deleted from memory after use.

¹ <http://www.ietf.org/rfc/rfc4252.txt>

Data Item	Description
Master Crypto Officer Password	A minimum 8-character password used by the master crypto officers to authenticate to the console interface. A default 8 character password exists on the device but a new password (minimum 8 characters) is set using the ESM. An obfuscated, non-human readable, version of the password is stored in the file system. The limited operating environment does not provide access to operating system services to access the obfuscated password data. This password is zeroized according to DoD 5220.22-M when returning the module to the manufacturer for repair or replacement.
Seed Key	Triple DES 168 bit seed key used to initialize the ANSI X9.31 Pseudo RNG which is used to generate other cryptographic keys.
RNG Seed	OpenSSL uses /dev/random as a source of random numbers. The linux kernel initializes this pseudo device at system startup. /dev/random guarantees a high degree of entropy and blocks until it has the proper level of entropy. The FIPS-validated version of OpenSSL performs continual tests on the random numbers it uses.
Other Cryptographic Keys	
Receiver SSH Public Key	This RSA 2048-bit public key corresponds to the Receiver SSH Private Key described above. This public key is output from the module in plaintext form as it is used for the transfer of key material in the SSH protocol. This key is generated by the FIPS validated RNG (certificate #387) during manufacturing and can never be regenerated again. The key is stored in unencrypted format on an unencrypted disk partition. The public key is maintained in a self signed certificate. This key is zeroized according to DoD 5220.22-M when returning the module to the manufacturer for repair or replacement.
Default ESM SSH Public Key	RSA 2048-bit public key used for the initial identification of a managing ESM and transfer of key material in the SSH protocol. The key is generated off the module and is stored in unencrypted form in the file system on an unencrypted disk partition (in the authorized keys table) for initial authentication of ESM devices. This key is zeroized according to DoD 5220.22-M when returning the module to the manufacturer for repair or replacement.
Active ESM SSH Public Key	RSA 2048-bit public key used for the identification of a managing ESM and transfer of key material in the SSH protocol. The key is generated off the module and is stored in unencrypted form in the file system on an unencrypted disk partition (in the authorized keys table). This key is zeroized according to DoD 5220.22-M when returning the module to the manufacturer for repair or replacement.
Integrity Public Key	RSA 2048-bit public key used to verify the digital signature of stored hash values used for the software/firmware integrity test. The public key is in a self signed certificate stored in unencrypted form in the filesystem. This key is zeroized according to DoD 5220.22-M when returning the module to the manufacturer for repair or replacement.

7 Roles and Services

The module supports a master crypto officer role, a crypto officer role and user roles. The module has a single system administrator role that is designated as the master crypto officer role and that role has the username "root". The master crypto officer role may initialize and zeroize the module using the console port. Crypto officers access the device over the SSH channel and give commands to retrieve data, request data from 3rd party devices, reconfigure the module to interact with additional or fewer 3rd party devices, and perform key management operations.

Users access the device by sending plaintext event and alert data, NetFlow, sFlow, log data instrumentation, and raw network traffic to the Receiver using the management ports.

The module supports services that are available to module operators in the various roles. All of the services are described in detail in the module's user documentation. Table 8 shows the services available to the various roles.

Crypto officers access the device over the SSH channel, give commands to use the Receiver device features, and perform key management operations, all of which are referred to as the "Receiver Instrumentation" in table 8 below.

Table 8. Roles and Services

<i>Service</i>	<i>Master Crypto Officer</i>	<i>Crypto Officer</i>	<i>User</i>
Change password, Authenticate to Console Interface, Initialize Receiver, Key Receiver, Start system, Zeroize system	●		
Import Receiver Key, Receiver Instrumentation, Reboot system, Rekey Receiver, Shutdown system	●	●	
Send user data to the Receiver			●
Read Status via SSH (Show Status)	●	●	
Read Status via HTTP (port 4242)	●	●	
Read Status via Console (Show Status)	●		
Read FIPS self-test (Reboot and On Demand)	●	●	

Importing Device keys is available as part of the (device) registration process. Each / any Receiver must register with an ESM before communications can begin between the devices. This registration is performed by exchanging 'key' information. A unique key is assigned to a device for the purpose of identifying a 'valid' device to be registered. Once the Receiver is added, it is very important to key the device. Keying the device enables the ESM to communicate with the Receiver and ensures added security by ignoring all outside sources of communication.

Note: A key exported from a non-FIPS device cannot be imported to a device operating in FIPS mode, nor can a key exported from a FIPS device be imported to a non-FIPS device. If you attempt to perform this action when you are adding a device to the system, the "The file is invalid" error will appear.

This term 'Key' in this manner is not related to encryption keys and refers to device registration keys.

NitroSecurity uses the Linux 'shred' command as the actual 'process' to securely erase disk data following the guidelines under the authority of DoD Directive 5220.22-M for the protection of classified information. NitroSecurity also recommends its customers become familiar with the NIST Special Publication 800-88 (Guidelines for Media Sanitation) to devise an appropriate erasure policy specific to their environment.

The Linux 'shred' command is designed primarily to securely delete files on the system. Using 'shred' overwrites all addressable hard drive locations with a character, its complement, and then a random character, followed by verification. The procedure is completed a number of times and prevents data from being recovered by commercially available processes.

8 Access Control

Table 9 shows services that use or affect cryptographic keys or CSPs. For each service, the key or CSP is indicated along with the type of access.

- R** - The item is read or referenced by the service.
- W** - The item is written or updated by the service.
- E** - The item is executed by the service. (The item is used as part of a cryptographic service.)
- D** - The item is deleted by the service.
- Z** - The item is zeroized (DoD erasure according to DoD 5220.22-M) by the service.

Table 9. Access Control

Key or CSP	Service	Access Control
Default ESM SSH Public Key	Initialize Receiver	R,E
	Zeroize system	Z
Active ESM SSH Public Key	Key Receiver	W,E
	Receiver Instrumentation	R,E
	Zeroize system	Z
Receiver SSH Key Pair	Rekey Receiver	W,E
	Receiver Instrumentation	R, E,D
	Import Receiver Key	W
	Zeroize system	Z
SSH AES Encryption Key	Receiver Instrumentation	D,W,E
	Shutdown system	D
	Reboot system	D
HMAC Key	Receiver Instrumentation	D,W,E
	Shutdown system	D
	Reboot system	D
Integrity Public Key	Start system	E
	Zeroize system	Z
Crypto Officer Password	Change password	W,D
	Authenticate to Console Interface	R
	Zeroize system	Z
RNG Seed Key	Receiver Instrumentation, Key Receiver, Reboot system, Rekey Receiver, Shutdown system , Start	W,R,E,D

Key or CSP	Service	Access Control
	system, Zeroize system	

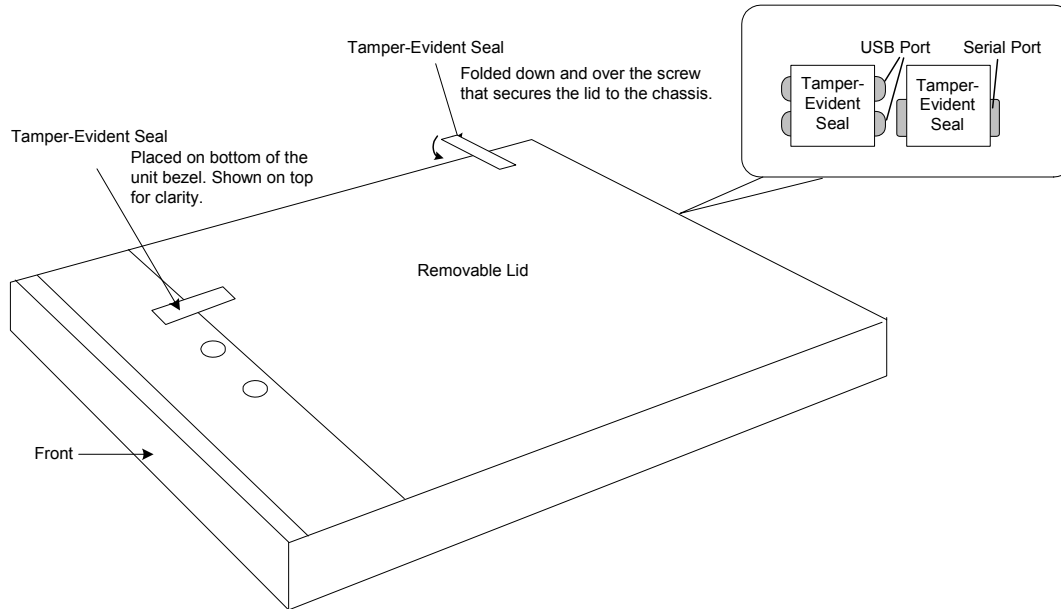
9 Physical Security

The physical security of the cryptographic module meets FIPS 140-2 level 2 requirements. The cryptographic module consists of production-grade components that include standard passivation techniques (a sealing coat applied over the module's circuitry to protect against environmental or other physical damage). The module meets commercial-grade specifications for power, temperature, reliability, shock and vibration.

The module has two tamper-evident seals that are serialized so they can be tracked by the crypto officer. One is placed over the seam where the top removable lid slides forward under the chassis top cover. The other seal is placed over the rear seam between the top cover and the rear panel. The top cover is removed by sliding it back and then lifting it off. This action breaks both seals, leaving evidence of tampering. The crypto officer guidance directs the crypto officer to periodically inspect the module for signs of tampering such as dents or scratches on the module enclosure or damage to the tamper evident seals. If tampering is detected, the crypto officer is instructed to perform a zeroize command and then to contact NitroSecurity Technical support for further assistance.

Figure 7 shows how the tamper evident seals are placed over the front and rear seams between the module's removable lid and the module chassis. A crypto officer applies a tamper evident seal (provided with the module) over the USB connectors to prevent their use without leaving evidence of tampering. These seals must be inspected in accordance with the organization security policy.

Figure 7. Tamper Evident Seals.



10 Self Tests

The module performs both power-on self test (POST) and conditional self tests to verify the integrity and correct operational functioning of the cryptographic module. If the system fails a self test, it reports status indicating that a failure has occurred and transitions to an error state, blocking all data input, data output and control input via their respective interfaces.

While the module is performing any power on self test or conditional test, software rules within the executable image prevent the module from entering a state where data output via the data output interface is possible.

Anyone with physical or logical access to the module can run the POST on demand by power cycling the module or entering a Reboot command.

Table 10 summarizes the system self tests and conditional tests.

Table 10. Self Tests.

<i>Self Test</i>	<i>Description</i>
<i>Mandatory power-up tests performed at power-up and on demand:</i>	
Cryptographic Algorithm Known Answer Tests	Each cryptographic algorithm (AES, Triple-DES, SHA-1, and RNG) performed by the module, is tested using a "known answer" test to verify the correct operation of the algorithm.
Firmware Integrity Test	The module verifies the RSA 2048 bit digital signatures on SHA-1 hashes of the NitroSecurity Software (Version 8.0.0.20080605) to confirm their integrity.
<i>Critical Functions tests performed at power-up:</i>	
None	No security-relevant critical functions tests are performed.
<i>Conditional tests performed, as needed, during operation:</i>	
Pairwise Consistency Tests	The module performs pairwise consistency tests whenever RSA asymmetric keys are generated.
Continuous RNG	16 bits continuous testing is performed during each use of the approved RNG. This test is a "stuck at" test to check the RNG output data for failure to a constant value.

Any self test success or failure messages are output to error log files.

Known answer tests for encryption/decryption or hashing, function by encrypting or hashing a string for which the calculated output is known and stored within the cryptographic module. An encryption or hashing test passes when the freshly calculated output matches the expected (stored) value. A test fails when the calculated output does not match the expected value. For decryption, the test then decrypts the ciphertext encrypted string. A decryption test passes when the freshly calculated output matches the plaintext value. A decryption test fails when the calculated output does not match the plaintext value.

Known answer tests for Random Number Generators function by seeding the RNG with known values and checking that the output matches the pre-calculated value stored within the cryptographic module. The test passes when the freshly generated output matches the pre-calculated value. A test fails when the generated output does not match the pre-calculated value.

Pairwise consistency tests for RSA keys (these keys are used for key transport) use the public key to encrypt a plaintext value. The resulting ciphertext value is compared to the original plaintext value. If the two values are equal, then the test fails. If the two values differ, the private key is used to decrypt the ciphertext and the resulting value is compared to the original plaintext value. If the two values are not equal, the test fails.

11 Mitigation of Attacks

The cryptographic module is not designed to mitigate specific attacks such as differential power analysis or timing attacks.

12 References

National Institute of Standards and Technology, *FIPS PUB 140-2: Security Requirements for Cryptographic Modules*, available at URL: <http://www.nist.gov/groups/stm/cmvp/>.

National Institute of Standards and Technology, *FIPS 140-2 Annex A: Approved Security Functions*, available at URL: <http://www.nist.gov/groups/stm/cmvp/>.

National Institute of Standards and Technology, *FIPS 140-2 Annex B: Approved Protection Profiles*, available at URL: <http://www.nist.gov/groups/stm/cmvp/>.

National Institute of Standards and Technology, *FIPS 140-2 Annex C: Approved Random Number Generators*, available at URL: <http://www.nist.gov/groups/stm/cmvp/>.

National Institute of Standards and Technology, *FIPS 140-2 Annex D: Approved Key Establishment Techniques*, available at URL: <http://www.nist.gov/groups/stm/cmvp/>.

National Institute of Standards and Technology and Communications Security Establishment, *Derived Test Requirements (DTR) for FIPS PUB 140-2, Security Requirements for Cryptographic Modules*, available at URL: <http://www.nist.gov/groups/stm/cmvp/>.

National Institute of Standards and Technology, *Data Encryption Standard (DES)*, Federal Information Processing Standards Publication 46-3, available at URL: <http://www.nist.gov/groups/stm/cmvp/>.

National Institute of Standards and Technology, *DES Modes of Operation*, Federal Information Processing Standards Publication 81, available at URL: <http://www.nist.gov/groups/stm/cmvp/>.

National Institute of Standards and Technology, *Digital Signature Standard (DSS)*, Federal Information Processing Standards Publication 186-2, available at URL: <http://www.nist.gov/groups/stm/cmvp/>.

National Institute of Standards and Technology, *Secure Hash Standard (SHS)*, Federal Information Processing Standards Publication 180-1, available at URL: <http://www.nist.gov/groups/stm/cmvp/>.