VORMETRIC

# *CoreGuard Security Server Cryptographic Module Security Policy*

*Document Version 1.2*
*July 23, 2004*

Table of Contents

# 1. Module Overview

The CoreGuard Security Server is a multi-chip standalone cryptographic module (Part Number 30, Hardware Release 1.0 Version 3.0, Sofware Version VN.3.0SP1-Build0060 and VN.3.0SP1-Build0064) encased in a hard opaque commercial grade metal case, with tamper evident seals. The cryptographic boundary is defined as the module's enclosure. The primary purpose for this module is to provide centralized security control of a configured policy. The diagram below illustrates the cryptographic module.

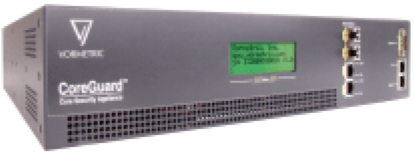

**Figure 1 – CoreGuard Security Server Cryptographic Module**

# 2. Security Level

The cryptographic module meets the overall requirements applicable to Level 2 security of FIPS 140-2.

**Table 1 - Module Security Level Specification**

| Security Requirements Section | Level |
|---|---|
| Cryptographic Module Specification | 2 |
| Module Ports and Interfaces | 3 |
| Roles, Services and Authentication | 3 |
| Finite State Model | 2 |
| Physical Security | 2 |
| Operational Environment | N/A |
| Cryptographic Key Management | 3 |
| EMI/EMC | 3 |
| Self-Tests | 2 |
| Design Assurance | 3 |
| Mitigation of Other Attacks | N/A |

# 3. Modes of Operation

## 3.1 Approved mode of operation

The CoreGuard Security Server supports a FIPS Approved mode of operation. The module is set into this mode via the "FIPS Mode" service, using the following steps:

1) The Master Admin must first authenticate to the module (as described in Section 7 below).
2) The Master Admin must then execute the system/fips enable command.

The module provides a status indicator informing the operator that the module is in a FIPS Approved mode of operation. The module provides the following status indicators when successfully set into the Approved mode of operation:

- "FIPS Enable Success" message via the CLI.
- A watermark in the background of the GUI is provided, indicating "FIPS Mode."

In the FIPS Approved mode of operation, the cryptographic module supports the following FIPS Approved algorithms:

- RSA 4096 bit encrypt/decrypt (key wrapping only)
- RSA 1024 and 2048 bit sign/verify per PKCS #1
- SHA-1
- AES (128 bit and 256 bit key length)
- Triple-DES (keying option 1; three unique keys)
- HMAC SHA-1

The cryptographic module uses 4096 bit RSA keys for key wrapping; 4096 bit RSA provides an equivalent strength of more than 128 bits of security.

The cryptographic module supports the following non-FIPS Approved algorithms:

- Diffie-Hellman 2048 (key agreement). .
- MD5 to support the TLS key establishment protocol.

The cryptographic module supports the following commercially available protocols:

- TLS V1.0 protocol for key establishment and secure communication when managing the module.
- SSH V2.0 protocol for secure communication when managing the module.

The cryptographic module relies on the implemented deterministic random number generator (DRNG) that is compliant with ANSI X9.31.

# 4. Ports and Interfaces

The CoreGuard Security Server cryptographic module provides the following physical ports and logical interfaces:

**Table 2 - Module Physical Ports and Logical Interfaces**

| Port Name | Interface Description | Port to Interface Mapping |
|---|---|---|
| NIC 1 (Fiber) | Fiber Optics<br>This port handles network traffic. When this port is enabled, NIC 1 (Copper) is disabled. | Data Input<br>Data Output<br>Status Output |
| NIC 2 (Fiber) | Fiber Optics<br>This port handles network traffic. When this port is enabled, NIC 2 (Copper) is disabled. | Data Input<br>Data Output<br>Status Output |
| NIC 1 (Copper) | Copper (RJ45)<br>This port handles network traffic. When this port is enabled, NIC 1 (Fiber) is disabled. | Data Input<br>Data Output<br>Status Output |
| NIC 2 (Copper) | Copper (RJ45)<br>This port handles network traffic. When this port is enabled, NIC 2 (Fiber) is disabled. | Data Input<br>Data Output<br>Status Output |
| MNGT | Copper RJ45 10Meg – 1Gig<br>This port is a dedicated port for management by an administrator, either locally or remotely; requires SSH or TLS connection through this port. | Control Input<br>Data Input<br>Data Output<br>Status Output |
| HA | Copper RJ45 10Meg – 1Gig<br>This port is a high availability port used for redundant interconnections to form what appears to an operator as a single highly available system when it is actually a cluster of systems. | Control Input<br>Data Input<br>Data Output<br>Status Output |
| Console Port | RS232 serial port<br>This port is a dedicated port for management by an administrator within a local environment. | Control Input<br>Data Input<br>Data Output<br>Status Output |
| 8 Network LEDs | Two LEDs for each network port to provide network status. | Status Output |
| 2 Power LEDs | An LED that provides power supply status. | Status Output |
| LCD | A display that provides status to an operator. | Status Output |
| Buzzer | An audible beeping sound that is emitted if any of the two power supplies fails. | Status Output |
| Power Supply | Two hot swappable power supplies. | Power |
| Zeroization Switch | A button that triggers zeroization of all plaintext CSPs when pressed. | Control Input |
| Power Cycle Switch | A switch that cycles the module's power when pressed. | Control Input |

| Port Name | Interface Description | Port to Interface Mapping |
|---|---|---|
| Power Alarm Reset Button | When one of the two power supplies fails, the module emits a constant beeping sound. When pressed, this button resets the alarm and stops the beeping. | Control Input |

# 5. Access Control Policy

## 5.1 Roles and Services

The CoreGuard Security Server cryptographic module supports five distinct operator roles, which are as follows:

- Master Admin (FIPS 140-2 Crypto-Officer): This role provides all of the services necessary to configure both the network and security attributes of the module.
- Security Admin (FIPS 140-2 User): This role provides all of the services necessary to configure the security attributes of the module.
- Network Admin: This role provides all of the services necessary to configure the network attributes of the module.
- HA role: The High Availability (HA) role is accessed by peer CoreGuard Security Server cryptographic modules and provides all of the services necessary to facilitate network redundancy.
- PEM role: The Policy Enforcement Module (PEM) role is accessed by host devices residing on the network and provides all of the services necessary to enforce the file access control and file protection capabilities.

**Table 3.1 - Specification of Master, Security, and Network AdminService Inputs & Outputs**

| Service Name | Service Description | Access Rights | | |
|---|---|---|---|---|
| | | Master | Security | Network |
| Network Configuration | Set, modify or delete network-related configuration items, eg., ip link, ip address, ip route, sslport, dns, ping, scan, traceroute, rping, arp. | X | | X |
| SetInfo | Allows the setting of host name, host owner, contact information, and location for the system. | X | | X |
| SetEmail | Sets email address, SMTP IP address, the polling interval for events, and enables or disables email notification of events on the system. | X | X | X |

| Service Name | Service Description | Access Rights | | |
|---|---|---|---|---|
| | | Master | Security | Network |
| SysLog | Allows sending of log messages in syslog format to external or remote machines. | X | X | X |
| Shutdown | Shuts down the module. | X | | X |
| Reboot | Forces a reboot of the module. | X | | X |
| SNMPTrap | Sets the Simple Network Management Protocol (SNMP) and sends event messages to the SNMPTrap manager. | X | X | X |
| FIPS Mode | Enables or disables the FIPS mode of operation. Disabling FIPS mode causes the cryptographic module to zeroize all CSPs stored within the crypto boundary before switching to non-FIPS mode. | X | | X |
| Config | Allows export of the configuration of the system and the complete set of cryptographic keys to a file which can be exported. | X | X | X |
| NTPDate | Sets or displays the NTP service on the system. | X | | X |
| Date | Sets or displays the date on the system. | X | | X |
| Time | Sets or displays the time on the system using a 24-hour clock. | X | | X |
| Zone Time | Sets the system time zone. | X | | X |
| Logging | Configures the events that are saved to a log file and displays what events were logged. | X | X | X |
| User Config | Allows adding, modifying, deleting, and displaying of operators on the system. | X | X | X |

| Service Name | Service Description | Access Rights | | |
|---|---|---|---|---|
| | | Master | Security | Network |
| Encryption Key Config | Allows adding, deleting, and listing of all the names and types of the stored cryptographic keys. | X | X | |
| Policy Config | Constructs the data access policies. This permits deleting policies, copying policies, setting alarm notification, showing policy information, and saving policy configurations. | X | X | |
| Add SA Config | Adds a new security association (SA), which defines the module's protection rules. | X | X | X |
| Delete SA Config | Removes a SA and the associated SA Master Key. | X | X | X |
| Modify SA Config | Applies or removes a policy associated with the SA. | X | X | X |
| Show SA Config | Displays SA information. | X | X | X |
| Add Host Config | Adds a new host. | X | X | X |
| Delete Host Config | Removes a host. | X | X | X |
| Modify Host Config | Permits users to configure the host. | X | X | X |
| Sign Host Config | Deletes and views signatures from applications or programs defined in a signature reference | X | X | |
| Show Host Config | Displays the host information. | X | X | X |
| HA Config | Enables redundant systems by configuring high availability (HA) hosts and interfaces. The module may also be removed from the HA cluster via this service; removing the module from the HA cluster will result in the destruction of all HA related keys. | X | | X |

| Service Name | Service Description | Access Rights | | |
|---|---|---|---|---|
| | | Master | Security | Network |
| Import Peer HA RSA Public Key | Permits loading of a peer's HA RSA Public Key from a file. | X | | |
| Export HA RSA Public Key | Permits the export of the HA RSA Public key to a file. | X | | |
| Import Config | Permits the import of key files, user files, network configurations, or the entire module configuration files. | X | X | X |
| Export Config | Permits the export of key files, user files, or the entire module configuration files. | X | X | X |
| Firmware Upgrade | Upgrades the Vormetric firmware into the module; the RSA digital signature is verified before accepting the upgraded firmware. | X | | X |
| Policy Composer | Tool to assist in creating a policy for the module to operate. | X | X | |
| Upload Policy | Imports policy files. | X | X | |
| Download Policy | Exports policy files. | X | X | |
| New Envelope Key | Generates a public/private Configuration RSA Key Pair. It also allows export of this key. | X | X | |
| Generate Certificate | Generates the CoreGuard RSA key pair and creates a X.509 self-signed certificate. | X | X | X |
| Download Certificate | Exports the CoreGuard RSA public key as an X.509 certificate. | X | X | X |
| System Log Retrieve | Exports the System Log. | X | X | X |
| About Vormetric | Displays the version number of the Vormetric module. | X | X | X |

**Table 3.2 - Specification of HA and PEM Service Inputs & Outputs**

| Service Name | Service Description | Access Rights | |
|---|---|---|---|
| | | HA | PEM |
| High Availability | The cryptographic module mirrors all of its configuration information amongst a given set of peer CoreGuard Security Server Cryptographic Modules currently alive on the network. | X | |
| File Protection | The remote PEM host submits files to the cryptographic module for encryption/decryption via an ESP connection. | | X |
| File & Software Access Control | The cryptographic module enforces file and software access restrictions on the remote PEM host. | | X |
| PEM Self-Protection Control | The cryptographic module controls the ability to upgrade or remove the PEM software on the remote PEM host. | | X |

In addition, the cryptographic module also supports the following unauthenticated services which do not disclose, modify, substitute cryptographic keys, use Approved security functions, or otherwise affect the security of the module:

- Self-tests: the cryptographic module performs all of the power-up self-tests upon power cycle.
- Unauthenticated status: the cryptographic module provides status via the LCD, LEDs, and the Buzzer.
- Zeroize via “Zeroization Switch”: the cryptographic module actively overwrites all of the CSPs stored within the crypto boundary when the “Zeroization Switch” on the chassis is depressed; this requires the physical presence of a human operator.

## 5.2 Definition of Critical Security Parameters (CSPs)

The following are CSPs contained in the module:

- Passwords: This is the Master Admin, Security Admin, and Network Admin passwords.
- SA Password: SA password controls access to those roles that can modify the security association.
- SA Master Key: TDES key used to encrypt host tokens, which are host records. This key is only used to support legacy systems.
- Session Encryption Key: This is an AES key used to encrypt data within the ESP tunnel.
- Diffie-Hellman Private Component: Used during the Diffie-Hellman negotiation for Session Encryption Keys.

- SA RSA Private Key: RSA private key used to sign the module's public portion of the Diffie-Hellman parameters when establishing the ESP Tunnel.
- Data Contents Encryption Key: A TDES or AES key that is used to encrypt/decrypt the data contents for the host.
- Configuration Encryption Key: TDES key used to encrypt/decrypt other cryptographic keys and configuration data that is exported/imported from/to the cryptographic module.
- Configuration RSA Private Key: RSA private key that is used to decrypt Configuration Encryption Keys during key establishment.
- HMAC Key: HMAC SHA-1key used in the ESP Tunnel for data integrity.
- HA Configuration Encryption Key: TDES key used to encrypt all HA traffic.
- HA RSA Private Key: RSA private key used to decrypt the HA Configuration Encryption Key during key establishment.
- HA RSA Signing Private Key: RSA private key used to sign HA messages.
- CoreGuard RSA Private Key: RSA private key used to sign host configuration messages.
- TLS RSA Private Key: RSA private key used to authenticate the handshake process between the client and CoreGuard Security Server.
- TLS Encryption Key: AES or TDES key used to encrypt/decrypt the communication channel between the client and CoreGuard Security Server.
- TLS HMAC Key: HMAC SHA-1key used in the TLS tunnel for data integrity.
- SSH RSA Private Keys: RSA private key used to authenticate the handshake process between client and CoreGuard Security Server.
- SSH Encryption Key: AES or TDES key used to encrypt the communication channel between client and CoreGuard Security Server.
- SSH HMAC Key: HMAC SHA-1 key used by SSH to provide data integrity.

## 5.3 Definition of Public Keys:

The following are the public keys contained in the module:

- Image Authentication Key: RSA public key used to verify the firmware's integrity.
- Diffie-Hellman Public Component: The public component during the Diffie-Hellman negotiation.
- SA RSA Public Key: RSA public key sent to and used by the host to verify the CoreGuard's public portion of the Diffie-Hellman key exchange when establishing the ESP Tunnel.
- Configuration RSA Public Key: RSA public key used to encrypt the Configuration Encryption Key during key establishment.
- HA RSA Public Key: RSA public key that is used to encrypt the HA Configuration Encryption Key during key establishment.
- HA RSA Signing Public Key: RSA public key used by peer's to verify HA messages sent by the CoreGuard Security Server.
- CoreGuard RSA Public Key: The public component of the CoreGuard RSA Private Key; the public key is used to verify the signed host configuration messages.
- TLS RSA Public Key: The public component of the TLS RSA Private Key; the public key is used by the client to verify the handshaking process between the client and the CoreGuard Security Server.

- SSH RSA Public Key: The public component of the SSH RSA Private Key; the public key is used to verify the handshaking process between the client and the CoreGuard Security Server.
- Host TLS RSA Public Key: This public key is used by the CoreGuard Security Server to verify the handshaking process between the host management interface and the CoreGuard Security Server.
- Host ESP RSA Public Key: RSA public key used to verify the public portion of the Diffie-Hellman key exchange coming from the host when establishing the ESP Tunnel.
- HA Peer RSA Signing Public Key: RSA public key used to verify HA messages sent by peer CoreGuard Security Servers.

## 5.4 Definition of CSPs Modes of Access

The table below defines the relationship between access to CSPs and different module services. The modes of access shown in the table are defined as follows:

- Generate: Creates the identified data item. If the data item is a cryptographic key, generation is performed using a FIPS Approved process (e.g., FIPS Approved DRNG).
- Input: Entry of data item.
- Output: Output of data item.
- Wrap: CSP is wrapped.
- Unwrap: CSP is unwrapped.
- Used: The key is used to encrypt, decrypt, sign, or verify; this is dependent on the key in reference.
- Destroy: Destruction.

**Table 4 – CSP Access Rights for all Services**

| Service Name | CSPs Accessed | Modes of Access |
|---|---|---|
| Network Configuration | None | None |
| SetInfo | None | None |
| SetEmail | None | None |
| SysLog | None | None |
| Shutdown | None | None |
| Reboot | None | None |
| SNMPTrap | None | None |
| Config | SA Master Key<br>SA RSA Private Key<br>Data Contents Encryption Key<br>Passwords (only the hash) | Input, Output, Wrap (with Configuration Encryption Key), Unwrap (with Configuration Encryption Key), Destroy |

| Service Name | CSPs Accessed | Modes of Access |
|---|---|---|
| | Configuration Encryption Key | Input, Output, Wrap (with Configuration RSA Public Key), Unwrap (with Configuration RSA Private Key), Destroy |
| | Configuration RSA Private Key | Generate, Input, Output, Wrap (with TLS), Unwrap (with TLS) |
| NTPDate | None | None |
| Date | None | None |
| Time | None | None |
| Zone Time | None | None |
| Logging | None | None |
| User Config | Password | Destroy, Input, Unwrap (with SSH or TLS) |
| Encryption Key Config | Data Contents Encryption Key | Generate, Input, Unwrap (with SSH or TLS), Destroy |
| Policy Config | None | None |
| Add SA Config | SA RSA Private Key<br>SA Master Key | Generated |
| Delete SA Config | SA RSA Private Key<br>SA Master Key<br>SA Password | Destroy |
| Modify SA Config | SA Password | Input, Unwrap (with SSH or TLS) |
| | SA Master Key | Used |
| Show SA Config | None | None |
| Add Host Config | CoreGuard RSA Private Key<br>TLS RSA Private Key<br>TLS Encryption Key<br>TLS HMAC Key | Used |
| Delete Host Config | None | None |

| Service Name | CSPs Accessed | Modes of Access |
|---|---|---|
| Modify Host Config | CoreGuard RSA Private Key<br>TLS RSA Private Key<br>TLS Encryption Key<br>TLS HMAC Key | Used |
| Sign Host Config | TLS RSA Private Key<br>TLS Encryption Key<br>TLS HMAC Key | Use |
| Show Host Config | None | None |
| HA Config | HA RSA Private Key | Generate, Destroy, Used |
| | HA Configuration Encryption Key | Generate, Input, Output, Wrap (with HA RSA Public Key), Unwrap (with HA RSA Private Key), Destroy |
| FIPS Mode | All CSPs (when disabling FIPS Approved mode) | Destroy (when disabling FIPS Approved mode) |
| Import Peer HA RSA Public Key | None | None |
| Export HA RSA Public Key | None | None |
| Import Config | SA Master Key<br>SA RSA Private Key<br>Data Contents Encryption Key<br>Password (only the hash) | Input, Output, Wrap (with Configuration Encryption Key), Unwrap (with Configuration Encryption Key) |
| Export Config | SA Master Key<br>SA RSA Private Key<br>Data Contents Encryption Key<br>Password (only the hash) | Input, Output, Wrap (with Configuration Encryption Key), Unwrap (with Configuration Encryption Key) |
| Firmware Upgrade | None | None |
| Policy Composer | None | None |
| Upload Policy | None | None |
| Download Policy | None | None |

| Service Name | CSPs Accessed | Modes of Access |
|---|---|---|
| New Envelope Key | Configuration RSA Private Key | Generate |
| | TLS RSA Private Keys<br>TLS Encryption Key<br>TLS HMAC Key | Used |
| Generate Certificate | CoreGuard RSA Private Key<br>TLS RSA Private Key | Generate |
| Download Certificate | None | None |
| System Log Retrieve | None | None |
| About Vormetric | None | None |
| High Availability | All CSPs | Input, Output, Used |
| File Protection | Data Content Encryption Key, Session Encryption Key, HMAC Key | Used |
| File & Software Access Control | HMAC Key, Session Encryption Key | Used |
| PEM Self-Protection Control | CoreGuard RSA Private Key | Used |
| Self-tests | None | None |
| Unauthenticated status | None | None |
| Zeroize via “Zeroization Switch” | All CSPs | Destroy |

# 6. Identification and Authentication Policy

The cryptographic module shall enforce the separation of roles using identity-based operator authentication. The Master Admin, Security Admin, and Network Admin must enter a username and its password to log in. The username is an alphanumeric string of one to thirty-one characters. The password is an alphanumeric string of six to thirty-one characters. Upon correct authentication, the role is selected based on the username of the operator. The cryptographic module does not provide any feedback of authentication data to an operator during authentication (e.g., no visible display of characters when entering a password).

The HA and PEM operators are authenticated by proving possession of the appropriate 1024 bit RSA private key, which is not stored in the cryptographic module.

At the end of a session, the operator must log-out; after 20 minutes of inactivity the cryptographic module automatically logs out all operators. Upon power off of the module, all previous authentications are cleared and are not retained.

**Table 5 - Roles and Required Identification and Authentication**

| Role | Type of Authentication | Authentication Data |
|---|---|---|
| Master Admin | Identity-based operator authentication | Username and Password |
| Security Admin | Identity-based operator authentication | Username and Password |
| Network Admin | Identity-based operator authentication | Username and Password |
| HA | Identity-based operator authentication | Proof of possession of 1024 bit RSA private key |
| PEM | Identity-based operator authentication | Proof of possession of 1024 bit RSA private key |

**Table 6 – Strengths of Authentication Mechanisms**

| Authentication Mechanism | Strength of Mechanism |
|---|---|
| Username and Password | In total, there are 62 character possibilities for the password. The module enforces a minimum password length of 6. Therefore, the probability that a random attempt will succeed or a false acceptance will occur is $1/62^6$, which is less than 1/1,000,000.<br>The maximum number of authentication attempts that can be made in a one minute period is 60; the module enforces this by forcing a one second delay per failed authentication attempt. The probability of successfully authenticating to the module within one minute is $60/62^6$, which is less than 1/100,000. |
| Proof of possession of 1024 bit RSA private key | A 1024 bit RSA private key can be expected to have no less than 80 bits of strength, and would require a minimum of $2^{80}$ operations to compromise the authentication procedure. As such probability that a random attempt will succeed or a false acceptance will occur is $1/2^{80}$ which is less than 1/1,000,000.<br>The cryptographic module can process at most, 52429 number of Ethernet frames in a one minute period. The probability of successfully authenticating to the module within one minute is $52429/2^{80}$ which is less than 1/100,000. |

# 7. Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the CoreGuard Security Server does not contain a modifiable operational environment. The cryptographic module only loads and executes code digitally signed by Vormetric using 1024 bit RSA.

# 8. Security Rules

The cryptographic module's design corresponds to the cryptographic module's security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 2 module.

## 8.1 FIPS 140-2 Imposed Security Rules

1. The cryptographic module shall provide five distinct operator roles. These roles include the FIPS 140-2 required User and Crypto-Officer roles.
2. The cryptographic module shall provide identity-based authentication.
3. The cryptographic module encrypts data using FIPS Approved algorithms, TDES and AES; this is determined by the configuration set by the Master Admin and Security Admin.
4. The cryptographic module shall perform the following tests:
    a. Power up Self-Tests:
        i. Cryptographic Algorithm Known Answer Tests:
            1. RSA encrypt/decrypt
            2. RSA sign/verify
            3. SHA-1
            4. AES
            5. Triple-DES
            6. HMAC-SHA-1
            7. Diffie-Hellman
            8. DRNG
        ii. Software Integrity Test (32 bit checksum)
        iii. Critical Function Test: N/A

    b. Conditional Self-Tests:
        i. Continuous Random Number Generator (RNG) test – performed on non-FIPS Approved RNG and the FIPS Approved DRNG
        ii. RSA pairwise consistency test (for both encrypt/decrypt and sign/verify)
        iii. Firmware Load test
5. Self-test can be performed by cycling power.
6. Upon failure of a self-test, the cryptographic module shall output an error message describing the specific error.

7. Data output shall be inhibited during key generation, self-tests, zeroization, and error states.
8. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
9. All imported public keys are protected within a X.509 certificate.

## 8.2 Vendor Imposed Security Rules

1. The module has a default Master Admin username and password upon first receiving the module.
2. The customer is required to change the default password for the Master Admin upon first accessing the module.
3. The default Master Admin cannot be changed.
4. The default Master Admin cannot be deleted.
5. A delay of one second between each login failure attempt is enforced by the module.

# 9. Physical Security Policy

## 9.1 Physical Security Mechanisms

The CoreGuard Security Server is a multi-chip standalone cryptographic module that includes production-grade components and a production-grade opaque enclosure with tamper evident seals placed on both sides of the module to indicate attempts at removing the cryptographic module's cover.

## 9.2 Operator Required Actions

The Master Admin is required to periodically inspect the tamper evident seals.

**Table 7 – Inspection/Testing of Physical Security Mechanisms**

| Physical Security Mechanisms | Recommended Frequency of Inspection/Test | Inspection/Test Guidance Details |
|---|---|---|
| Tamper Evident Seals | 3 months | The Master Admin is required to inspect the tamper evident seals for visible signs of malice. Upon viewing any suspicious characterisitcs of the seals, the Master Admin must assume that the device has been fully compromised. The Master Admin is required to zeroize the cryptographic module and shall return the device to the factory. |

# 10. Mitigation of Other Attacks Policy

The module was not designed to mitigate other specific attacks outside the scope of FIPS 140-2.

# 11. References

- FIPS PUB 140-2, May 25, 2001
- FIPS PUB 180-2, August 1, 2002
- FIPS PUB 46-3, October 25, 1999
- FIPS PUB 197, November 26, 2001

# 12. Definitions and Acronyms

| Acronyms | Definitions |
|---|---|
| **AES** | Advanced Encryption Standard |
| **ARP** | Address Resolution Protocol |
| **CSP** | Critical Security Parameter |
| **DRNG** | Deterministic Random Number Generator |
| **ESP** | Encapsulation Security Protocol |
| **FIPS** | Federal Information Processing Standards |
| **HA** | High Availability |
| **HMAC** | Hash Message Authentication Code |
| **ICMP** | Internet Control Message Protocol |
| **IP** | Internet Protocol |
| **LCD** | Liquid Crystal Display |
| **LED** | Light Emitting Diode |
| **MTU** | Maximum Transmission Unit |
| **NIC** | Network Interface Card |
| **NTP** | Network Time Protocol |
| **PEM** | Policy Enforcement Module |
| **RSA** | Rivest, Shamir, & Adelman |

| | |
|---|---|
| **SA** | Security Association |
| **SHA** | Secure Hash Algorithm |
| **SMTP** | Simple Mail Transfer Protocol |
| **SNMP** | Simple Network Management Protocol |
| **SSH** | Secure Shell |
| **TDES** | Triple Data Encryption Standard |
| **TLS** | Transport Layer Security |
| **USB** | Universal Serial Bus |