# Command Encryption Module Security Policy

Firmware Version: 1.1

Table of Contents

Page

**1. SCOPE OF DOCUMENT ..... 3**

**2. CRYPTOGRAPHIC MODULE SPECIFICATION ..... 3**

**3. MODULE PORTS AND INTERFACES ..... 4**

**4. ROLES, SERVICES, AND AUTHENTICATION ..... 4**

4.1 ACCESS CONTROL POLICY ..... 4
4.2 SERVICES ..... 4
4.3 CRYPTO OFFICER ROLE ..... 5
4.4 USER ROLE ..... 5

**5. PHYSICAL SECURITY ..... 5**

**6. KEY MANAGEMENT ..... 8**

6.1 KEY INPUT ..... 9
6.2 KEY STORAGE ..... 9
6.3 KEY ZEROIZATION ..... 9

**7. SELF-TEST ..... 9**

**8. SECURITY POLICY ..... 9**

**9. OPERATIONAL ENVIRONMENT ..... 10**

**10. MITIGATION OF OTHER ATTACKS ..... 10**

**11. SETUP AND INITIALIZATION PROCEDURES ..... 10**

## 1. Scope of Document

This document defines the security policy for the Command Encryption Module, also referenced as the cryptographic module. This security policy follows the requirements of Federal Information Processing Standards pubulication (FIPS) 140-2, Security Requirements for Cryptographic Modules.

## 2. Cryptographic Module Specification

The Module is a firmware module as defined by FIPS PUB 140-2 submitted for FIPS 140-2 Level 2 validation. The purpose of the cryptographic module (Module) is to encrypt the commands transmitted to other systems. The cryptographic module does not perform any other cryptographic function.

The Module is a Multi-Chip Standalone module as defined by FIPS PUB 140-2. The cryptographic boundary of the module is the case of the hardware computing platform.

**Table 1 Module Compliance Table**

| Security Requirements Section | Level |
|---|---|
| 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 | 3 |
| Self-Tests | 2 |
| Design Assurance | 2 |
| Mitigation of Other Attacks | N/A |
| Cryptographic Module Security Policy | 2 |
| Overall Level of validation | **2** |

## 3. Module Ports and Interfaces

The table below describes a mapping of logical interfaces to physical ports:

**Table 2 Mapping Logical Interfaces to Physical Ports**

| FIPS 140-2 Interface | Logical Interface | Physical Interface |
|---|---|---|
| Data Input Interface | Input parameters of module function calls | Ethernet/Network Port |
| Data Output Interface | Output parameters and return values of module function calls | Ethernet/Network Port |
| Control Input Interface | Module control function calls | Ethernet/Network Port |
| Status Output Interface | Return values from module status function calls | Monitor |
| Power Interface | Initialization function | Power Interface |

## 4. Roles, Services, and Authentication

### 4.1 Access Control Policy

The cryptographic module supports two roles: User and Crypto- Officer. Table 3 below describes the authenticaion mechanism:

**Table 3: Roles and Required Identification and Authentication**

| Approved Operators | Type of Authentication | Authentication Data | Strength of Authentication |
|---|---|---|---|
| User | Role Based | 24 bit Password | 1:16,777,216 in guessing the password |
| Crypto-Officer | Role Based | 8 alpha/numeric/special characters | The length of password has to be 8 characters. The characters contain alphabet, number, and special characters. Therefore the password has more than 6,095,689,385,410,816 (= 94^8) patterns. |

### 4.2 Services

The cryptographic module supports the services listed in table 4. The table groups the authorized services by the operator roles and identifies the Cryptographic Keys and CSPs associated with the services. The access type is also identified per service.

**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 function.)

**Table 4: Services for Authorized for Roles**

| Role | Authorized Services | Cryptographic Keys and CSPs | Access Type |
|---|---|---|---|
| Crypto-Officer | Setup and Initialization | Password | Write, Execute |
| | Run Self Tests | None | Execute |
| | Change Own Password | Password | Write, Execute |
| | View Audit Data | None | Read |
| | Zeroization | Triple-DES | Write |
| | Show Status | None | Read |
| User | Symmetric Encryption | Triple-DES key | Execute |
| | Key Change | Triple-DES key, Password | Write, Execute |
| | Show Status | None | Read |
| | Change Own Password | Password | Write, Execute |

### 4.3 Crypto Officer role

Setup and Initialization: The Crypto-Officer is responsible for the secure setup and initialization of the module. This includes inputting the cryptographic keys from ROM reader, turnning on the key change service, turnning on the encryption service, change password, and set physical secuirty parameters.

Run Self-Tests: The module is located in a locked rackmount cabinet with access only by the Crypto-Officer. The Crypto-Officer must unlock the cabinet to power-on the device to run all self-tests automatically.

Change Own Password: The Crypto-Officer can change their own password.

View Audit Data: The Crypto-Officer can view the encryption start and stop logs and view the key change logs.

Zeroization: The Crypto-Officer can perform the zeroization of all keys by issuing the zeroize service or by formatting the hard drive.

Show Status: The Crypto-Officer can view the status of the symmetric encryption service.

### 4.4 User Role

Symmetric Encryption: The User can perform symmetric encryption of command data signals input into the module.

Key Change: The User role can issue the key change command to force a key change for the Module.

Show Status: The User can view status of the key change service.

Change Own Password: The User can change their own password.

## 5. Physical Security

The Module was tested on a HP Compaq DC 5100 hardware computing platform with the following configuration:

- Intel® Pentium® IV 640 3.2 GHz Processor
- 512 MB DDR2-533MHz RAM DIMM
- 80Gb Disk Drive

- 48x CD Drive
- Intel® 915GV Express Chipset
- 3.5” (3Mode 720kb/1.20MB/1.44MB) Floppy Disk Drive
- Broadcom NetXtreme Gigabit Ethernet Controller
- Broadcom 5782 PCI LAN Controller
- RS-232C D-Sub 9 PIN
- RGB Mini D-Sub 15 PIN (Monitor Port)
- 8 – USB 2.0 ports (2 in Front, 6 in Rear)
- Intel® Graphics Media Accelerator 900 Controller
- Flash ROM
- 2 – PS/2 Compatible 6 PIN Mini DIN
- 2 - Speaker Port (1 in Front, 1 in Rear)
- 2 – Stereo Mini Port (1 in Front, 1 in Rear)

The Modules removable cover and ports are sealed with tamper evidence seals. The module is stored in a cabinet with mechanical lock such as combination dial lock that is only known to the Crypto-Officer.

The Module has tamper evident seals that cover all external physical ports that are installed as part of the setup and initialization procedure. The location of the seals are described below:


Figure 1 Front


Figure 2 Back


Figure 3 Left Side

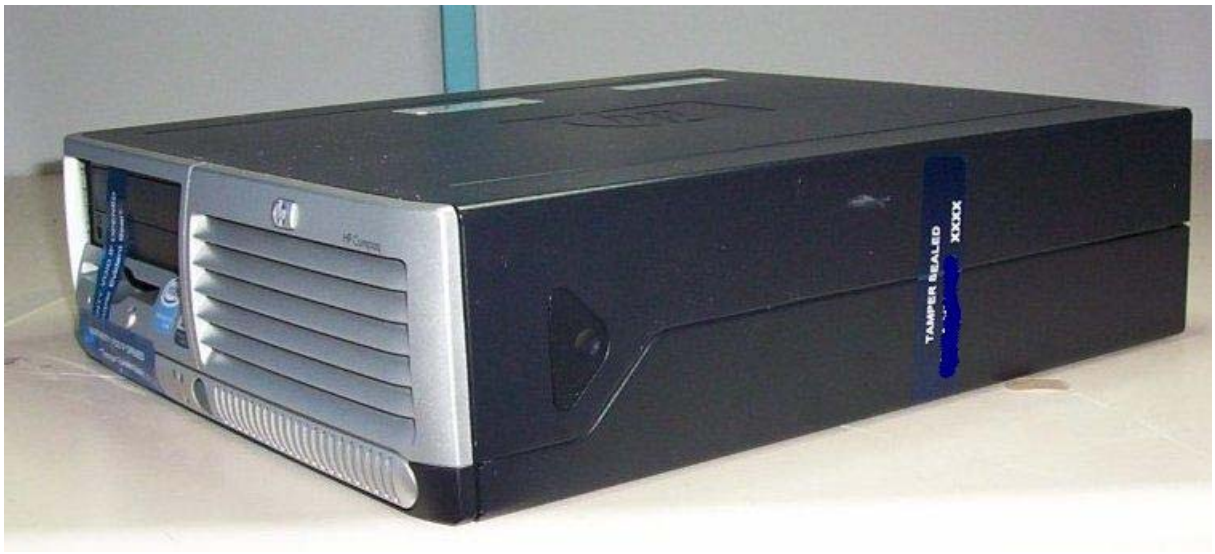


Figure 4 Right Side

The Inspection/Testing of Physical Security Mechanisms of the Module is shown in table 5.

**Table 5: Inspection/Testing of Physical Security Mechanisms**

| Physical Security Mechanisms | Recommended Frequency of Inspection/Test | Inspection/Test Guidance Details |
|---|---|---|
| Tamper evident Seals | • Once a day: During operation<br>• Once a month: Others | Compare the record with the condition of tamper evident seal |
| Rack with Combination dial lock | • Once a day: During operation<br>• Once a month: Others | Compare the record with the condition of combination lock number |

## 6. Key Management and CSP's

The Module employs the Triple-DES encryption. Characteristics of Triple-DES implemented in the Module are as follows:

- CFB (Cipher Feed Back) Mode
- EDE (Encryption-Decryption-Encryption) Mode
- 3 independent keys

The algorithm certificate number is 759.

**Table 6: Keys and CSP Table**

| Key and CSP | CSP Type | Storage | Use | Role |
|---|---|---|---|---|
| Symmetric Keys | Triple-DES | Plaintext | Data encryption | User |
| Password | Password | Plaintext | Authentication | User, CO |

### 6.1 Key Input

As the module does not support key generation, keys are input into the Module via the ROM reader through the serial port as part of the setup and initialization procedure. Keys are never input or output while the Module is operational.

### 6.2 Key Storage

Keys are stored in the hard drive when keys are input from ROM reader. A key is temporarily stored in RAM during a encryption state. When power is removed from the Module the key in RAM is destroyed.

### 6.3 Key Zeroization

Each key can be zeroized by using the zeroization command or by formatting the hard disk drive. This command is allocated to the Crypto Officer. All keys and CSP's are also zeroized by formatting the hard drive of the Module. Formatting the hard drive is allocated to the Crypto-Officer role.

## 7. Self-Test

The Module performs power-up self-tests as follows when the Module is power up.

- Software/firmware integrity test. This is the CRC 32 peformed on the Module.
- Cryptographic algorithm test. This is the known answer test for Triple DES CFB mode for encryption only.

And the above mentioned power-up tests can perform if authenticated operator requires the tests on demand.

## 8. Security Policy

The Module provides the following security policy:

1) Crypto Officer is responsible for secure setup and initialization of the Module.
2) Only one Crypto-Officer is defined for the Module.
3) The Crypto-Officer is the only Role with physical access to the Module.
4) When the module has been configured, the Crypto-Officer must remove the keyboard and mouse and install tamper evident seals over the exposed ports (USB, Parallel, floppy, microphone, audio, and CD drive)
5) If tamper seals are removed, keys must be zerozied and the module must be reinitialized with new keys and any seals that have been destroyed must be replaced. Before any tamper seal can be replaced, the surface must be cleaned and a new tamper seal must be reapplied.
6) Password for the Crypto-Officer must be at least 8 alpha/numeric and special characters long. The Crypto-Officer account must locked out after 10 failed login attempts.

## 9. Operational Environment

The operational environment is non-modifiable.

The Module integrity is protected by disconnecting keyboard and mouse after the application has been configured and loaded with keys, and also all of the open physical ports and the covers/doors are sealed with tamper evident seals. The hardware platform is also secured in a combination locked cabinet when operational. The operating system also has a firewall installed to prevent remote access to the Module. The module is never connected to the Internet.

## 10. Mitigation of Other Attacks

The Module will not implement security mechanisms to mitigate the other attacks.

## 11. Setup and Initialization Procedures

When the Module has been received from the factory, the following procedures must be performed in order to configure the module in FIPS Mode of operation:

1. The Crypto-Officer must configure a firewall to permit remote access only for IP address and dedicated TCP ports of the Server and deny any other remote access. The procedures for configuring the firewall rules can be found in the Command Encryption Module Installation Guidance document.
2. The Crypto-Officer must authenticate to the module and connect the ROM reader to the hardware platform via the serial port
3. The Crypto-Officer must load the triple-DES encryption keys
4. The Crypto-Officer must turn on the key change service
5. The Crypto-Officer must turn on the Encryption Service
6. The Crypto-Officer must disconnect the mouse and keyboard and insert tamper seals over the USB, Parallel, floppy, microphone, audio, and CD drive ports
7. The User must send the authenticated Key Change command from the Server to initialize the key into memory.
8. The User must view that the encryption key has been successfully initialized.