Command Encryption Module Non-proprietary Security Policy

Firmware Version: 3.0

Table of Contents

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 publication (FIPS PUB) 140-2, Security Requirements for Cryptographic Modules.

2. Cryptographic Module Specification

The cryptographic module (Module) is a firmware module as defined by FIPS PUB 140-2 submitted for FIPS 140-2 Level 2 validation. The purpose of the Module is to encrypt the commands transmitted to other systems. The 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 Ethernet/Network Port
Power Interface	Initialization function	Power Interface

4. Roles, Services, and Authentication

4.1 Access Control Policy

The Module supports two roles: User and Crypto-Officer. Table 3 below describes the authentication 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	14 alpha/numeric/special characters	The length of password has to be 14 characters. The characters contain alphabet, number, and special characters. Therefore the password has more than 4,205,231,901,698,742,834,534,301,696 (= 94^14) patterns.

4.2 Services

The 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.)

N/A – There is no access to the cryptographic keys and CSPs by the service.

Table 4: Services for Authorized for Roles

Role	Authorized Services	Cryptographic Keys and CSPs	Access Type
Crypto-Officer	Setup and Initialization	Password	R, W, E
	Run Self Tests	None	N/A
	Change Own Password	Password	R, W, E
	View Audit Data	None	N/A
	Key Zeroization	Triple-DES key	W
	Module Zeroization	Triple-DES key, Password	W
	Show Status	None	N/A
User	Symmetric Encryption	Triple-DES key, Password	R, E
	Key Change	Triple-DES key, Password	R, E
	Show Status	None	N/A

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, turning on the key change service, turning on the encryption service, change password, and set physical security 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 or power-cycle the Module 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.

Key Zeroization: The Crypto-Officer can perform the zeroization of all keys by issuing the zeroize service.

Module Zeroization: The Crypto-Officer can perform the zeroization of all keys and CSPs by overwriting the hard drive.

Show Status: The Crypto-Officer can view the status of the symmetric encryption service. The Module status can be observed by power cycling the PC.

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.

5. Physical Security

The Module was tested on a HP ProDesk 600 SFF STD G2 hardware computing platform with the following configuration:

- Windows 7 Enterprise SP1
- Windows Firewall with Advanced Security Version 6.1
- Intel® Core i5® 6500 3.2 GHz Processor
- 4GB DDR4-2133MHz SDRAM DIMM
- 200 Watt power supply
- 500GB Disk Drive
- 16x DVD-ROM Drive
- Intel® Q150 Chipset
- Intel® HD Graphics 530
- Intel® I219LM Gigabit Ethernet Controller
- RS-232C D-Sub 9 PIN
- RGB Mini D-Sub 15 PIN (Monitor Port)
- 2 - DVI (Display Port)
- 6 – USB 3.0 ports (2 in Front, 4 in Rear)
- 4 – USB 2.0 ports (2 in Front, 2 in Rear)
- 2 – PS/2 Compatible 6 PIN Mini DIN
- 4 – Stereo Mini Port (2 in Front, 2 in Rear)
- 4 – Filler panels in Rear

The Module's removable cover and all external physical ports except the ports used in FIPS 140-2 mode (RGB Mini D-Sub 15 PIN Monitor port and Ethernet RJ45 port) are protected with 6 tamper evident seals (Part Number: MSS-FIPS-16-500) as part of the setup and initialization procedure. The tamper evident seals shall be installed for the module to operate in a FIPS Approved mode of operation.

Figures 1, 2, 3 and 4 indicate the exact locations of the tamper evident seals. Note that one seal (#4) is split 2/3 and attached at left of the RGB Mini D-Sub 15 PIN Monitor port and another seal (#5 and 6) is split half and attached at right of the RGB Mini D-Sub 15 PIN Monitor port and Ethernet RJ45 port, to allow the use of these ports in FIPS 140-2 mode.

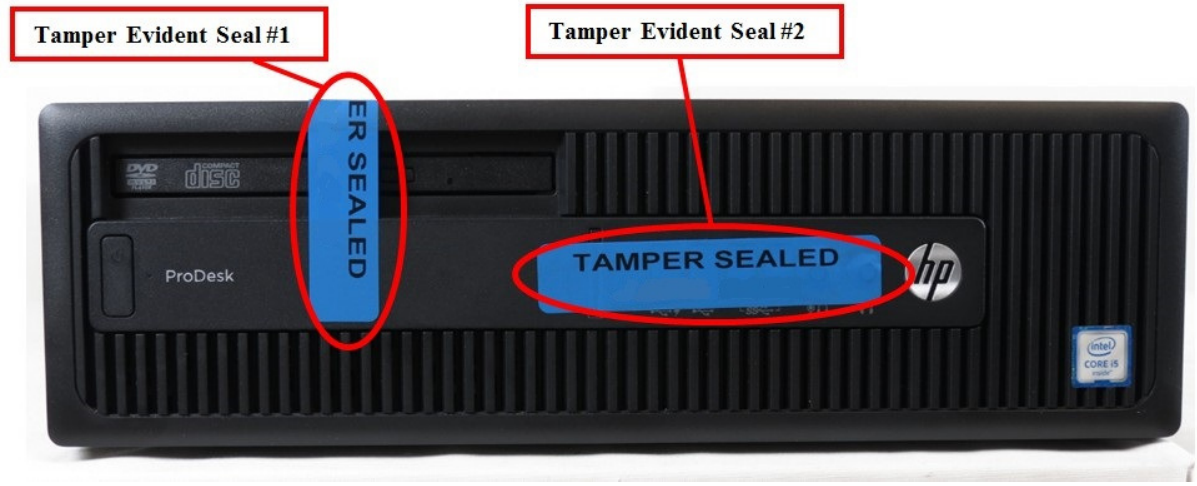

Figure 1 Front

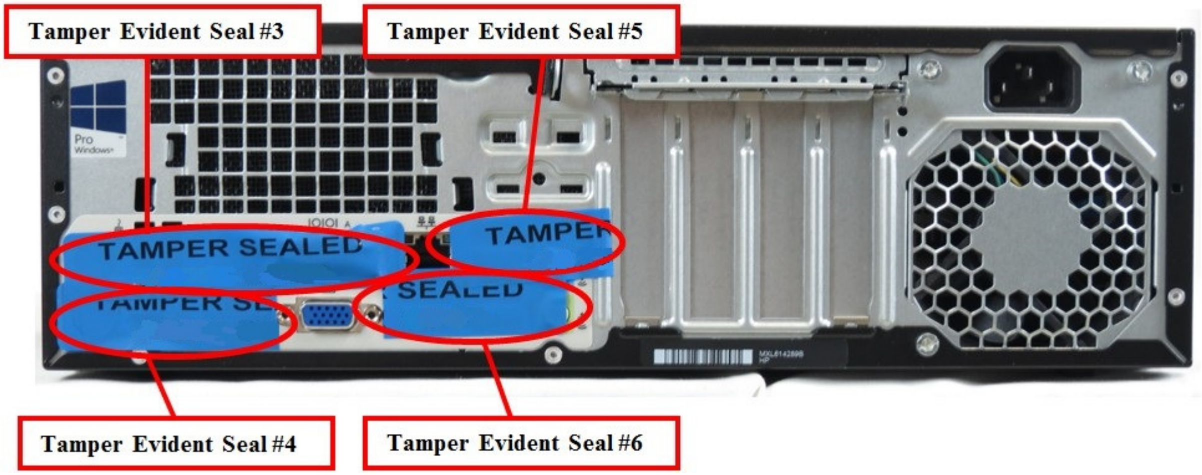

Figure 2 Rear

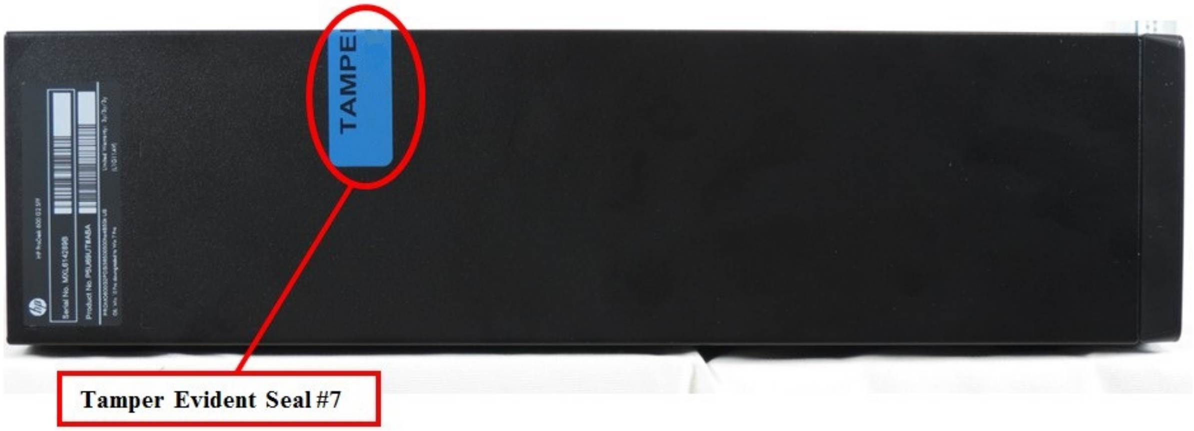

Figure 3 Left Side

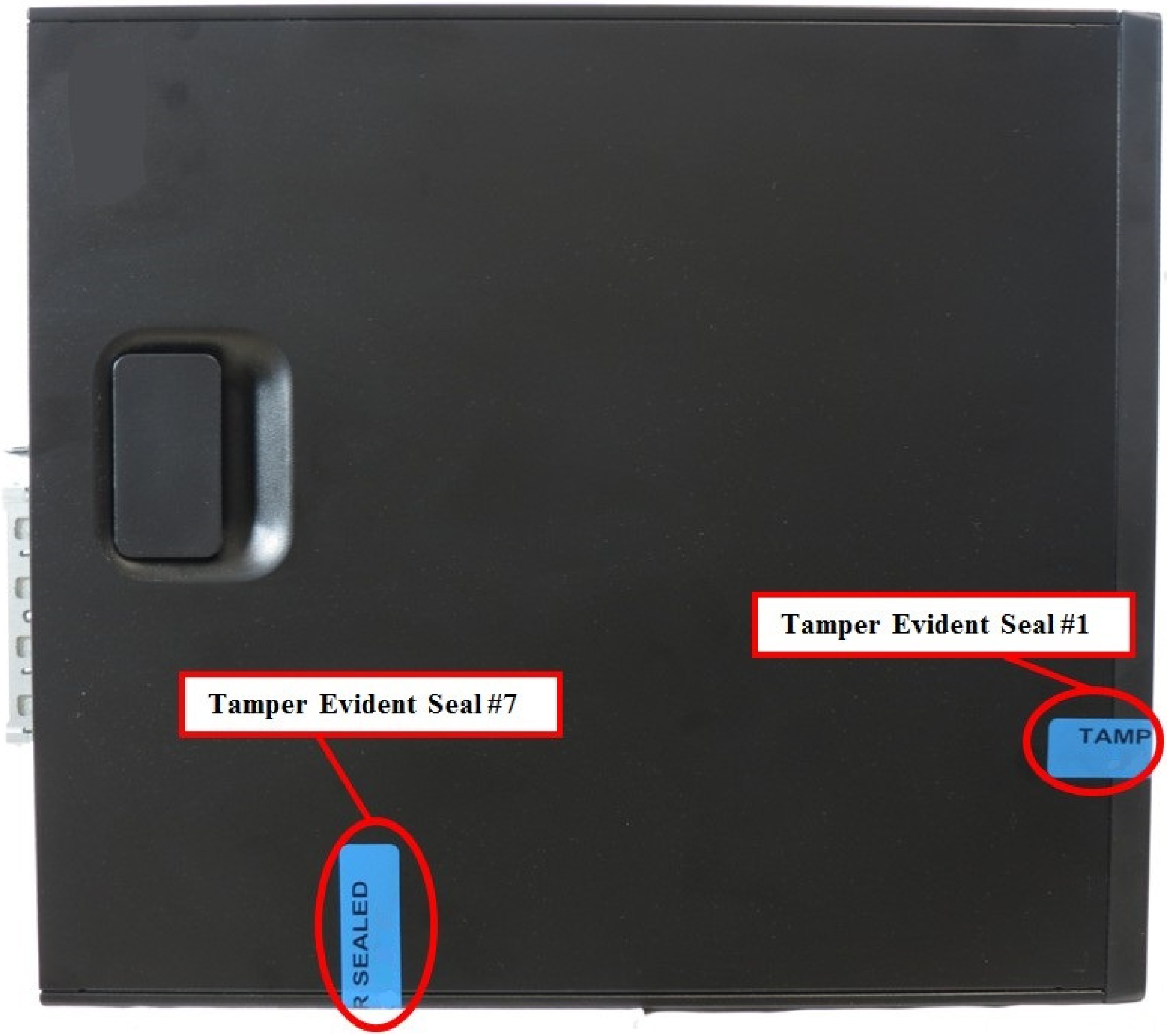

Figure 4 Top

There is no tamper evident seal on the left side.

The filler panels that cover the unpopulated slots on the back of the chassis shown in Figure 2 cannot be removed without opening the top cover, which is protected with a tamper evident seal as shown in Figure 3 and 4.

To replace a tamper evident seal, all traces of the previously removed seal must be first eliminated. The surface must be cleaned with a solution consisting of alcohol and distilled water in the areas where the tamper evident seals are to be applied. The seals must be applied on clean and dry surfaces only.

It is the responsibility of the Crypto Officer to perform the inspection and testing of the physical security mechanisms as described in Table 5.

Also, it is the responsibility of the Crypto Officer to secure and have control of any unused seals.

Refer to the Crypto Officer Guidance document for information on how to order new tamper evident labels.

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 operations • Once a month: Others	Compare the record with the condition of tamper evident seal
Rack with Combination dial lock	• Once a day: During operations • 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 shown in the Table 6.

Table 6: Approved Algorithms

CAVP Cert	Algorithm	Standard	Mode/ Method	Key Lengths, Curves or Moduli	Use
2191	Triple-DES	SP 800-67	Cipher Feed Back (CFB)	3 independent 64 bit keys	Data Encryption

Table 7: 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 USB on PC 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 key zeroization command. This command is allocated to the Crypto-Officer. All persistently-stored keys and CSPs can be zeroized by uninstalling the cryptographic module software and securely overwriting the hard drive. The secure overwrite process is allocated to the Crypto-Officer role and must be performed by or under the direct supervision of the Crypto-Officer.

7. Self-Test

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

- Software/firmware integrity test. This is the Error Detection Code (EDC) performed 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, Serial, Stereo Mini Port and DVD drive)
5) If tamper seals are removed, keys must be zeroized 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 14 alpha/numeric and special characters long. The Crypto-Officer account must be locked out after 6 failed login attempts for 10 minutes.

9. Operational Environment

The operational environment is non-modifiable.

The Module integrity is protected by disconnecting the ROM reader, 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 is also configured with logical controls such as a local security policy and a firewall 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 a FIPS Approved mode of operation:

1. The Crypto-Officer must be authenticated to the Module by using the default password which has been set at the factory.
2. The Crypto-Officer must configure a new password for the module which meets the policy requirements specified in the Command Encryption Module Installation Guidance document.
3. 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 incoming or outgoing connections. The procedures for configuring the firewall rules can be found in the Command Encryption Module Installation Guidance document.
4. The Crypto-Officer must connect the ROM reader to the hardware platform via the USB port.
5. The Crypto-Officer must load the triple-DES encryption keys.
6. The Crypto-Officer must turn on the key change service.
7. The Crypto-Officer must turn on the Encryption Service.
8. The Crypto-Officer must disconnect the ROM reader, mouse and keyboard and insert tamper seals over the USB, Serial, Stereo Mini Port and DVD drive ports.
9. The User must send the authenticated Change Key command from the Server to initialize the key into memory.
10. The User must view that the encryption key has been successfully initialized.
11. It is the User's responsibility to verify that the module returns "Encryption key update success" in order to confirm the encryption key change completed successfully.

Upon completion, the Module is considered initialized and only operates in a FIPS Approved mode of operation: