HEWLETT-PACKARD TIPPINGPOINT

FIPS 140-2 NON-PROPRIETARY SECURITY POLICY

HP TippingPoint Security Management System

Level 1 Validation
Firmware Version: 3.2.0.8312.3

Document Version: 1.03

FIPS 140-2 Non-Proprietary Security Policy

HP TippingPoint Security Management System

Contents

List of Figures

List of Tables

1. Introduction

This document is a non-proprietary Cryptographic Module Security Policy for the HP TippingPoint Security Management System Firmware version 3.2.0.8312.3.

Federal Information Processing Standards (FIPS) 140-2, *Security Requirements for Cryptographic Modules*, specifies the U.S. and Canadian Governments' requirements for cryptographic modules. The following pages describe how HP TippingPoint's SMS meets these requirements and how to use the SMS in a mode of operation compliant with FIPS 140-2. This policy was prepared as part of the Level 1 FIPS 140-2 validation of the HP TippingPoint Security Management System.

More information about FIPS 140-2 and the Cryptographic Module Validation Program (CMVP) is available at the website of the National Institute of Standards and Technology (NIST): http://csrc.nist.gov/groups/STM/cmvp/index.html.

In this document, the HP TippingPoint Security Management System is referred to as the *SMS, TippingPoint SMS, the module, the firmware* or the *SMS module*.

1.1 Purpose

This document covers the secure operation of the HP TippingPoint SMS firmware module including the initialization, roles, and responsibilities of operating the product in a secure, FIPS-compliant manner.

1.2 References

This Security Policy deals specifically with the operation and implementation of the module in the technical terms of the FIPS 140-2 standard. Additional information on the module can be found on the HP TippingPoint website.

1.3 Definitions and Acronyms

Table 2: Definitions and Acronyms

Term/Acronym	Description
AES	Advanced Encryption Standard
CLI	Command Line Interface
CSP	Critical Security Parameter
DES	Data Encryption Standard
DH	Diffie Hellman
DRNG	Deterministic Random Number Generator
FIPS	Federal Information Processing Standard
GUI	Graphical User Interface
HMAC	Hash-based Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure

IPS	Intrusion Prevention System
MD5	Message Digest 5
RNG	Random Number Generator
RSA	Public Key encryption developed by RSA Data Security, Inc. (Rivest, Shamir and Adleman)
SHA	Secure Hash Algorithm
SMS	Security Management System
SRDI	Security Relevant Data Item
SSH	Secure Shell
SSL	Secure Sockets Layer
TDES	Triple Data Encryption Standard
TLS	Transport Layer Security
TP	TippingPoint

2 Module Specifications

2.1 Overview

The TippingPoint SMS serves as the control center where one can configure, monitor, and report on multiple TippingPoint devices in your network. Each SMS can manage up to 150 TippingPoint devices (based on environmental conditions). The TippingPoint SMS module is a centralized management solution for managing and monitoring a deployment of TippingPoint security devices. The SMS module provides cryptographic services for communicating with the security devices and user interfaces.

For FIPS 140-2 purposes, the TippingPoint SMS is considered a cryptographic firmware module. The physical embodiment is multi-chip standalone.

A typical network-wide TippingPoint deployment consisting of a centralized TippingPoint Security Management System (SMS) managing multiple TippingPoint systems is depicted in Figure 1.

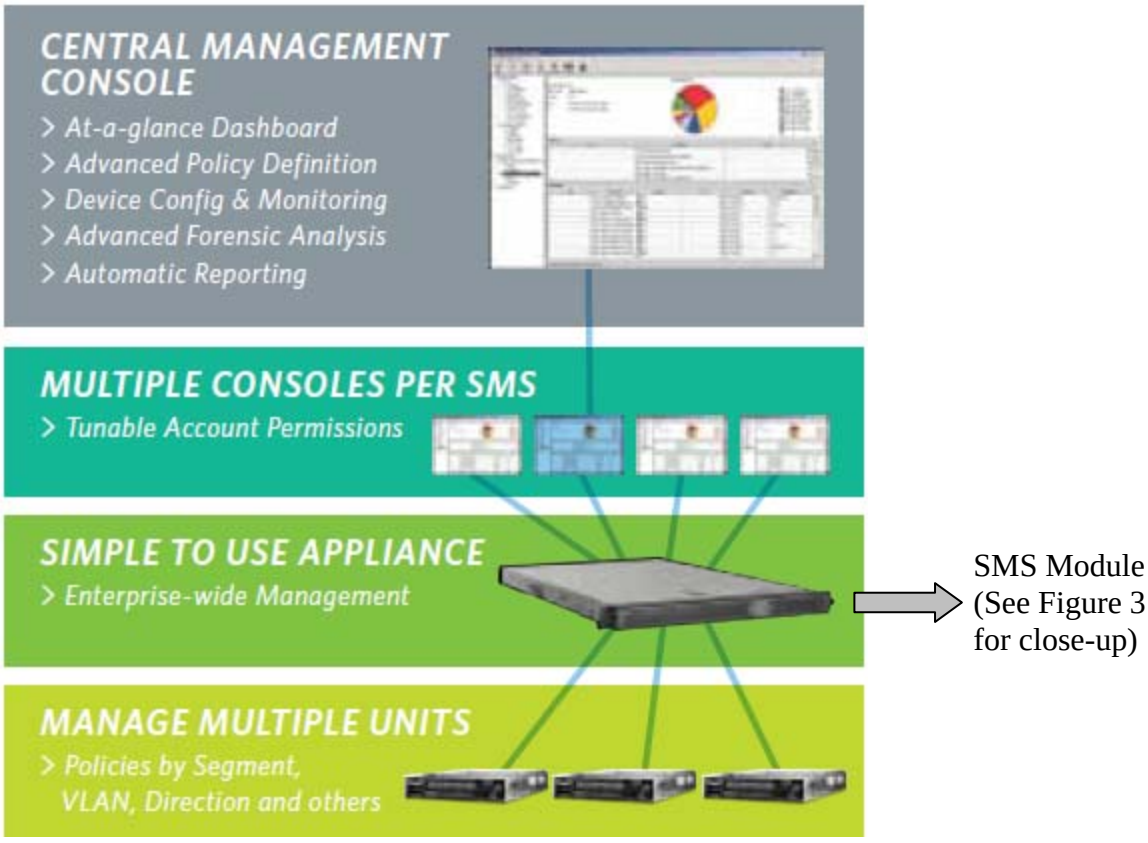

Figure 1: SMS Module in HP TippingPoint Architecture

2.2 Test Configuration

The TippingPoint SMS firmware module was tested for FIPS 140-2 overall Level 1 compliance using the following configuration:

Table 1: Test Configuration

SMS Firmware Version	Processor	Test Hardware	Operating System
3.2.0.8312.3	Intel Xeon	HP ProLiant DL320 G6 Server	Fedora Core 10

The SMS module can be operated in FIPS-approved mode as well as in non-FIPS mode. The module offers the option of three FIPS modes: Disable, Crypto and Full. Only the 'Full' FIPS mode is considered the FIPS-approved mode of operation. The other two 'Disable' and 'Crypto' modes are considered non-FIPS approved modes of operation. For all FIPS 140-2 purposes, all instances of 'FIPS-mode' or 'FIPS-approved mode' refer only to 'Full' FIPS mode on the module.

The SMS module allows updates only with packages that are signed by TippingPoint's private key, so it has a limited operational environment.

When operated in FIPS mode, the TippingPoint SMS Cryptographic module meets the overall requirements applicable to Level 1 security of FIPS 140-2. Table 2 shows each of the FIPS 140-2 sections and the corresponding levels that the SMS module meets the requirements for.

Table 2: SMS Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services and Authentication	3
Finite State Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
EMI/EMC	1
Self Tests	1
Design Assurance	2
Mitigation of Other Attacks	N/A

2.2 Cryptographic Boundary

The logical cryptographic boundary is the SMS firmware binary comprising of all the logical components within the firmware. None of the logical components within the firmware are excluded from the FIPS 140-2 security requirements.

The module's physical cryptographic boundary is the entire physical enclosure of the test appliance used as the SMS Server i.e. the platform where the SMS firmware and the Operating System reside.

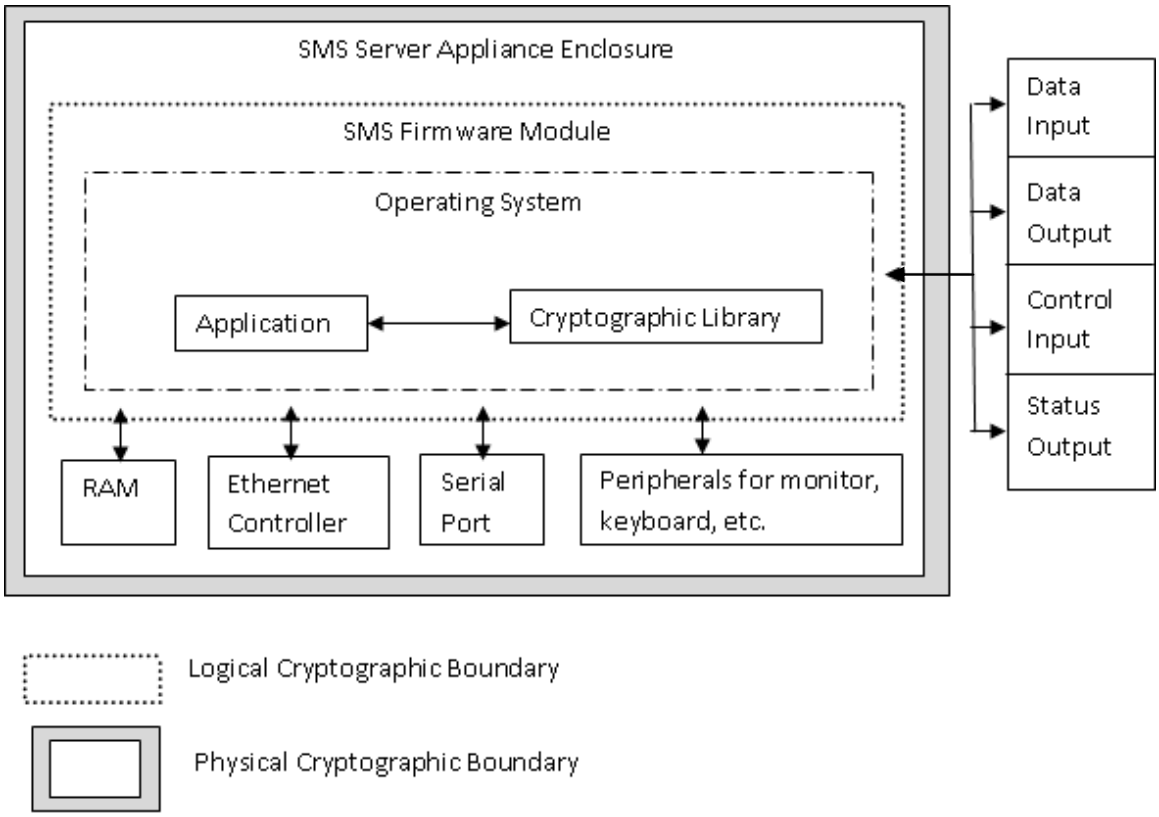

Figure 2: Cryptographic Boundary

The below figure shows the hardware used for testing the SMS firmware module against the FIPS 140-2 security requirements. The entire outer enclosure of this appliance (encompassing the top, bottom, left, right, front and rear faces) represents the physical cryptographic boundary of the module.

Figure 3: Hardware used for testing

2.3 Ports and Interfaces

Table 3 lists the ports and interfaces of the module and their mapping to the corresponding FIPS 140-2 logical interfaces. The physical ports correspond to the physical ports of the test appliance that executes the SMS firmware module, and the module interfaces correspond to the logical functions or APIs of the module.

The mouse port provided on the test appliance used to execute the SMS firmware is unused and has no use in FIPS or in Non-FIPS mode. The System Identification (UID) button has a LED integrated in the button and there is one such button on the front and the back side of the appliance used for testing. When one of these buttons is pressed, the blue LED in both of these buttons turns on and only serves the purpose of helping in locating the appliance when placed in an appliance rack.

The following table describes the module ports and interfaces.

Table 3: Ports and Interfaces

FIPS 140-2 Logical Interfaces	Module Interfaces	Physical Ports of the test appliance (HP ProLiant DL320 G6 Server)
Data Input	Input parameters of module's function calls.	Ethernet Management Port, Auxiliary Ethernet Management Port, RS-232 Serial Port, Keyboard Connector, USB port
Data Output	Output parameters of module's function calls.	Ethernet Management Port, Auxiliary Ethernet Management Port, RS-232 Serial Port, VGA Monitor port
Control Input	Module's function calls	Ethernet Management Port, RS-232 Serial Port, USB Ports, Keyboard Connector, Power/Reset Button, CD-ROM port
Status Output	Return codes of module's function calls	Ethernet Management Port, RS-232 Serial Port, VGA Monitor port, Ethernet port LEDs, Power LED, System Identification (UID) Button
Power Input	N/A	Power Port

3 Roles, Services and Authentication

3.1 Roles

The SMS module can be accessed in any one of the following ways:

- CLI over the Server appliance's serial port.
- CLI using the Server appliance's Monitor and Keyboard port.
- CLI using SSH over Server appliance's Ethernet Management port
- CLI using Telnet over Server appliance's Ethernet Management port
- SMS Client GUI using TLS over Server appliance's Ethernet Management port.
- SMS Web GUI using TLS over Server appliance's Ethernet Management port. When configured to not require passwords, the SMS Web GUI allows non-cryptography relevant services such as downloading of the SMS Client software, downloading SMS User Guide without requiring operator authentication. This TLS GUI always requires operator authentication for viewing system logs or other reports generated on the module. No other management or configuration task is possible over this web GUI.
- Remote authentication using RADIUS or Active Directory Server. Before remote authentication can be used, it is required that this service be enabled on the module and the username be added in the User List (without the password) and be assigned one of the roles. Without this procedure, the module will not authenticate an operator even if correct username and password are entered for remote authentication.

Telnet and HTTP are not allowed to be used in FIPS mode.

For each of the above access methods, the TippingPoint SMS supports identity-based authentication, where each user has a name and password. An access level is associated with each user. There are 3 user access levels as shown in the table below.

Table 4: SMS User Roles

User Access Level	Description	FIPS Role
Operator	Can only perform cryptographic services over TLS using SMS Homepage and SMS Client. Operator primarily has read-only access to the configuration settings. An operator can modify his own password and load a new TLS RSA key pair signed with the TippingPoint's private key.	User
Administrator	Can only perform cryptographic services over TLS using SMS Homepage and SMS Client. Administrator can modify some configuration settings. An administrator can modify his own password and load a new TLS RSA key pair signed with the TippingPoint's private key.	User

Super-User	Can access Console CLI, SSH CLI, TLS (SMS Homepage and SMS Client) and modify all configuration settings. Only a super-user can add and delete users and modify any user's password and access level. Also, only a super-user can configure the box for FIPS mode and disable FIPS mode. Only a Super-User can perform software updates.	Crypto-Officer

3.2 Services

The table below shows the services provided by the SMS and the access level required to perform them for each of the roles supported by the module.

Table 5: Services

Operator	Admin	Super User	Service	Service Inputs	Service Outputs	Notes
		Y	Enable/disable FIPS-approved 'Full-FIPS' mode	GUI option select	Module reboot	
Y	Y	Y	View FIPS Mode status	CLI command or GUI option select	FIPS mode status	Only Super-User has access to CLI
		Y	View self-test failure log file	SMS Client GUI option	fips-selftest-failure.log file	
Y	Y	Y	Configure own password	New password over CLI or SMS Client	Success or failure notification	Only Super-User has access to CLI
		Y	Configure any operator's password and access level	Username and new password and new access level over CLI or SMS Client	Success or failure notification	
		Y	Add/delete users	CLI command or GUI option select	None	
		Y	Configure	CLI	Success or	

			'password security level' for usernames and passwords	command and level desired	failure notification	
		Y	Install new firmware or software patch	New package and SMS Client GUI option select	Success or failure notification and reboot	
	Y	Y	Import or download non-cryptography relevant software package	New package and SMS Client GUI option or SSH CLI command	Success or failure notification	Packages are associated with IPS rules and traffic filtering and are non-cryptography relevant. Only Super-User has access to CLI.
		Y	Activate or delete non-cryptography relevant software package	SMS Client GUI option select or SSH CLI command	None	
	Y	Y	Reboot	Ctrl+Alt+Del at CLI or reboot CLI command or reboot SMS Client GUI option or via SMS Homepage	None	Only Super-User has access to CLI. Reboot can also be done unauthenticated by power cycling the test appliance.
Y	Y	Y	Perform FIPS power-up self-tests	None	Success indicator if all tests pass. If any test fails, error message is logged and module reboots.	Performed automatically during initialization at every boot-up.
Y	Y	Y	Install new TLS RSA key pair during	Vendor-supplied and signed TLS	Success or failure notification	This upload is possible only during FIPS-

			transition to FIPS mode	RSA key pair input using SMS Homepage	and reboot on success	mode enabling procedure.
		Y	Login to CLI and perform services over console or SSH	Username and password	CLI prompt if successful. Login prompt if unsuccessful	
Y	Y	Y	Login to SMS Homepage and view System logs and reports over TLS	Username and password	SMS Homepage if successful. Login screen if unsuccessful	
Y	Y	Y	Login to SMS Client GUI and perform services over TLS	Username and password	SMS Client GUI if successful. Login screen if unsuccessful	
	Y	Y	Configure non-FIPS related admin level settings	CLI command or SMS Client GUI option select	None	Only Super-User has access to CLI
		Y	Configure non-FIPS related super-user level settings	CLI command or SMS Client GUI option select	None	
Y	Y	Y	View non-FIPS related configuration	CLI command or SMS Client GUI option select	Configuration values	Only Super-User has access to CLI
Y	Y	Y	View non-FIPS related status	CLI command or SMS Client GUI option select	Status	Only Super-User has access to CLI

3.3 Unauthenticated Services

The SMS modules allow the following unauthenticated services:

Table 6: Unauthenticated Service

Service	Procedure	Service Inputs	Service Outputs
Power-up or Reboot the module	Power cycle or reboot using power button on the test appliance or using Ctrl+Alt+Del on module's console CLI	None	None
Perform power-up self-tests	Power cycle or reboot using power button on the test appliance or using Ctrl+Alt+Del on module's console CLI	None	Success or failure status indicator
Zeroize and regenerate ephemeral keys and CSPs	Power cycle or reboot using power button on the test appliance or using Ctrl+Alt+Del on module's console CLI	None	None
SNMP	Module automatically sends alert notifications if SNMP has been configured	None	Non-FIPS relevant data such as alerts, IPS network statistics. No key or CSP information is output by SNMP.
Disable FIPS-approved (Full FIPS) mode	Selecting the option during module boot-up sequence	None	No output. This procedure disables FIPS mode, zeroizes all keys, CSPs and security-relevant data.

3.4 Authentication Mechanisms and Strength

The TippingPoint SMS supports password authentication for users. A user must specify a name and password when authenticating over the CLI or SMS Client GUI or SMS Homepage.

The SMS module offers different levels for defining the required strength of usernames and passwords. These levels vary from 0 to 2, ranging from minimum to maximum restrictions on the usernames and passwords. Level 0 places no restrictions on the usernames and passwords. This level can be configured by the Super-User Crypto-Officer

to be anywhere between 0 and 2. This configurable level option on the module is referenced throughout this document as the ‘password security level’ and should not be confused with the FIPS 140-2 Level.

In Full FIPS mode, it is the Crypto-Officer’s responsibility to make sure that the module is configured to use ‘password security level’ of 1 or above for usernames and passwords. Thus, considering the lowest level 1, the password must be at least 8 characters. In the default configuration there is no restriction on what characters can be in the password. There are 95^8 possible passwords of the minimum length from the set of all displayable ASCII characters including space. The odds of randomly guessing a password of the minimum length would thus be 1 in 95^8 which is much less than 1 in 1,000,000.

The ‘password security level’ of 2 on the module requires level 1 restriction of 8-character passwords and additionally requires all passwords to have at least 2 letters, 1 number, and 1 non-alphanumeric character. This would reduce the number of possible passwords from the default settings. However, even with fixed values and positions for the required character classes, there would still be 95^4 possible passwords of the minimum length. The odds of randomly guessing the password for this fixed scenario would be 1 in 95^4, which is less than 1 in 1,000,000. Since the values and positions of the required character classes are not fixed, the number of possible passwords of the minimum length is larger. Thus the actual odds are even lower.

In the default configuration, a user account is locked for 5 minutes after 5 failed login attempts for that user. Thus the odds of randomly guessing a password with retries within one minute is 5 times the odds discussed above. That does not result in any odds larger than 1 in 100,000. The maximum number of retries can be configured up to 10, which would result in 10 times the odds discussed above, but this would still not result in odds larger than 1 in 100,000. To maintain FIPS compliance, the Crypto-Officer must not disable the configuration for account lockout on login failure or configure the lockout attempts to more than 5.

4 Secure Operation and Security Rules

In order to operate the TippingPoint SMS securely, the user should be aware of the security rules enforced by the module and should adhere to the physical security rules and secure operation rules and procedure.

4.1 Secure Operation

4.1.1 Enabling FIPS Mode

Before enabling FIPS mode ('Full' FIPS mode) on the module, the following should be verified:

- Verify that the SMS Client software has been downloaded on a computer in the same subnet as the appliance executing the SMS firmware. If the SMS Client has not been downloaded : On a computer in the same subnet as the appliance executing the SMS firmware, access the SMS Homepage (https://<IP address of SMS>) and download the SMS Client from the SMS Homepage.
- Verify that the version and patch level of the SMS module is FIPS compliant by accessing the SMS Client GUI and accessing 'Admin' category → 'General' tab. To ensure FIPS 140-2 compliance of the module, verify that the version listed in 'SMS Software' field is 3.2.0.8312 and the 'SMS Patches' field lists 3.2.0.8312.3 as the version currently installed. Only version number 3.2.0.8312.3 is a part of this validation.
- Contact HP TippingPoint and create an account on the Threat Management Center (TMC) website (https://tmc.tippingpoint.com) which will be required for installing vendor-signed FIPS keys onto the module.
- Verify the browsers and SSH clients used to connect to the SMS server support the Transport Layer Security (TLS) 1.0 protocol, sometimes referred to as SSL 3.1. TLS 1.0 support is required to connect to an SMS server running in FIPS mode.
- The Super-User should create BIOS password for the test appliance being used and maintain the security of this BIOS password to prevent unauthorized access.

After following the above steps and verifying all the above requirements, the SMS module should be placed in FIPS mode (denoted as 'Full' FIPS mode on the module) by a Crypto-officer by following the below procedure:

- Login to the SMS Client GUI with the Crypto-Officer authentication data created on the module.
- In the SMS Client GUI, access the '**Admin**' Navigation menu and then select '**Server Properties**'.
- If RADIUS or Active Directory servers were configured, then access the **Authentication** tab and under **RADIUS**, click on **'Reset'**. Also, under **Active Directory**, click on **'Edit'** and set all fields (except Port and Timeout) to '0000', click on **'OK'**. Under **Authentication Source**, select **'Edit'** and then select **'Use local authentication'** and click **OK**.

- Under the '**Management**' tab, in the '**Services**' section, make sure that HTTP and Telnet are unselected to disable these services. Then click **Apply**. As an alternative to this, the SMS CLI can be used to disable HTTP and Telnet by executing the following commands:
  "set svc.http-enable=no"
  "set svc.telnet-enable=no"
- In the '**FIPS Mode**' section, click **Edit**. Select '**Full-FIPS**' as the Requested State. On the same page, enter authentication information for a new SMS Crypto-Officer account with 'password security level' of 1 or above, which will be the only active account after the transition to Full-FIPS mode. This Crypto-Officer account and password should NOT match the credentials of any SMS account that existed prior to enabling Full-FIPS mode. Click **OK.** This will cause the module to reboot.
- Using a web browser, download FIPS keys for the SMS module from the Threat Management Center (TMC) website (https://tmc.tippingpoint.com) after a successful authentication and save this on the computer being used. This is an official TLS RSA key pair signed by TippingPoint. These FIPS keys are required to be imported into the module as part of the transition to Full-FIPS mode. Contact HP TippingPoint for any issues regarding this or for creating an account at the TMC website.
- After the SMS has rebooted, Crypto-Officer should access the SMS homepage or website (https://<IP address of SMS>) from any computer in the same subnet as the SMS and upload the official TLS key package to the SMS module. No other console operation should be performed at this stage. This FIPS key package has to be downloaded from the TMC website as explained in the above step.

The above procedure causes the SMS to do the following:

- Reboot
- Zeroize all keys and CSPs
- Generate new keys
- Perform FIPS power-up self tests
- Regenerate SSH and temporary TLS keys and certificates with associated conditional self-tests.
- Use the generated temporary TLS keys. SMS Client connections are not allowed at this stage. SMS web homepage only shows the option to upload the official TLS key pair at this stage.
- Reboot again after the official TLS key pair is imported via SMS Homepage using temporary TLS keys and the key package passes the associated conditional self-tests.
- Perform FIPS power-up self tests.
- Enter approved Full FIPS mode.
- Start using the new official TLS key pair.

These steps ensure that the FIPS requirements are met for doing self tests, not using the same keys and users in FIPS and non-FIPS modes, not allowing output during power-up

self tests, using only FIPS-approved cryptographic algorithms, etc. The SMS should now be operating in a FIPS compliant manner.

4.1.2 Current FIPS Mode

The current FIPS mode can be seen on the SMS GUI by accessing 'Admin' Navigation menu → 'Server Properties' → 'Management' tab → 'FIPS Mode' section. This FIPS mode status can be seen by all operators of all roles.

4.1.3 Other FIPS-related procedures

To force the FIPS power-up self tests to be rerun, an operator must reboot the SMS module.

To zeroize and regenerate all cryptographic keys in the module, a Crypto-Officer can disable and then re-enable FIPS mode through the GUI by following the procedure provided in Section 4.1.4 and 4.1.1 respectively.

4.1.4 Disabling FIPS mode

In order to disable the Full-FIPS mode, the following procedure should be followed. This is allowed only to the Crypto-Officer role.

- In the SMS Client GUI, access the '**Admin**' Navigation menu and then select '**Server Properties**'.
- If RADIUS or Active Directory servers were configured, then access the **Authentication** tab and under **RADIUS**, click on **'Reset'**. Also, under **Active Directory**, click on **'Edit'** and set all fields (except Port and Timeout) to '0000', click on **'OK'**. Under **Authentication Source**, select **'Edit'** and then select **'Use local authentication'** and click **OK**.
- Select the '**Management**' tab.
- In the '**FIPS Mode**' section, click **Edit**.
- Select '**Disabled**' as the Requested State.
- When prompted, create a new SuperUser account. All user accounts that existed prior to disabling FIPS mode will be deleted.

This procedure causes the SMS to perform the same steps as done when going into Full FIPS mode except that the module is put into disabled FIPS mode, the FIPS self-tests are no longer performed, and the module may use cryptographic algorithms not allowed by FIPS.

4.2 Self-Tests

The SMS Module performs the following power-up self-tests every time the module boots-up:

- Firmware Integrity Test using MD5
- AES KATs
- DRBG KAT and Health Tests
- DSA Sign/Verify
- HMAC-SHA KATs

- RNG ANSI X9.31 KAT
- RSA Sign/Verify
- SHA KATs
- Triple-DES KATs

The SMS module performs the following conditional self-tests every time the associated service is invoked:

- Continuous Random Number Generator Test for ANSI X9.31 RNG
- Continuous Random Number Generator Test for DRBG
- Pair-wise consistency tests for RSA (sign/verify, encrypt/decrypt)
- Pair-wise consistency test for DSA (sign/verify)
- Software Load Test : When a user attempts to update the firmware/software, verify that the new software file was signed by the TippingPoint's private key. If the signature check fails, the software update is aborted with no changes to the existing installed software. This validation is also done when FIPS mode is disabled.

On failing any of the power-up or conditional self-tests, the module logs the error message in the log file "fips-selftest-failure.log". The Crypto-Officer can access this failure log file by logging in to the module using the SMS Client and then accessing Tools → Diagnostics → Log Utils → sms-server → Create Logs Zip File. Then a filename and location on the local computer can be specified, where the zip file will be stored. This zip file will contain the fips-selftest-failure.log file which logs the self-test error message and the timestamp of the failure.

For all power-up and conditional self-test failures, except for the power-up firmware integrity test and the conditional software load test, the module immediately reboots itself.

In case of the power-up firmware integrity self-test failure, the module halts the boot process and an operator must then manually reboot the module. If case of a software load test failure, the module will reject and not install the incorrect file.

4.3 Security Rules

The security rules enforced by the TippingPoint SMS include both the security rules that TippingPoint has imposed and the security rules that result from the security requirements of FIPS 140-2.

4.3.1 FIPS 140-2 Security Rules

The following are the security rules derived from the FIPS 140-2 requirements when in full FIPS mode:

- The TippingPoint SMS module supports identity-based user authentication, access levels, and services as discussed in section 3.
- The TippingPoint SMS module supports CSPs and controls access to them as discussed in section 5.

- The TippingPoint SMS module has support for changing into or out of full FIPS mode, zeroizing/generating keys, etc. See section 4.1 for more information.
- When in full FIPS mode, only cryptographic algorithms allowed by FIPS are used. See section 5.1 for the list of algorithms.
- The TippingPoint SMS module performs the self tests as listed in Section 4.2.
- There is no data output from the SMS during the power-up self tests.
- The users do not have direct access to the internal storage on the SMS where the CSPs and installed software images are stored.
- All external entry of CSPs is encrypted with the exception of passwords entered over the console.
- The user is not allowed to configure the password settings for less than 8 characters.
- Telnet and HTTP are disabled/disallowed in Full FIPS mode.
- SSL 2.0 and SSL 3.0 support is disabled in Full FIPS mode. Only TLS 1.0/SSL 3.1 is allowed in this FIPS-approved mode.
- On enabling FIPS-approved mode, the module deletes the existing user database and adds the new default Super-User account as per the login information specified in the SMS GUI. It also removes all SMS backups and device snapshots stored on the SMS server and deletes all custom responder actions.

4.3.2 TippingPoint Security Rules

The following are the security rules that are enforced by TippingPoint when the SMS is in Full FIPS mode:

- For enabling FIPS mode, the SMS module should be placed in 'Full' FIPS mode.
- The external database replication feature cannot be enabled in FIPS-mode.
- The failed-lockout attempts counter must remain activated for all users and configured at incorrect attempts threshold of 5 or below.
- The 'password security level' setting for each SMS user should remain at or above Level 1.
- In Full FIPS mode, the SSH terminal will negotiate connections using only FIPS 140-2 approved algorithms.
- Restoring SMS backups that were created when SMS was not in Full-FIPS mode is not permitted by the module.
- Importing or executing custom Responder Actions is not allowed by the module.
- The use of custom web security SSL certificates is not permitted by the module.
- The SMS hardware appliance must have a BIOS password enabled and set.
- BIOS boot settings should not be edited while the module is operating in FIPS-approved mode and the appliance should boot only from the main hard drive.
- HTTP and Telnet are not allowed to be used in FIPS-approved mode of operation.
- While using RADIUS or Active Directory server for remote authentication to the SMS module, the operator is responsible for using a minimum of 8-character password and 8-character shared secret.
- The software patches and the FIPS key (TLS RSA key pair) packages must be obtained by the Crypto-Officer only via the secure TMC website

(https://tmc.tippingpoint.com) using TLS and the access will require an appropriate module owner's authentication.

- The SMS firmware module will be shipped already installed in a compatible appliance by HP TippingPoint.
- The firmware version 3.2.0.8312.3 is the only FIPS-validated version. Thus, the patch should not be rolled back after installation and no other firmware versions or patch versions should be installed into the module.
- The module allows the Crypto-Officer to select the option of not requiring authentication on the SMS Homepage (Web UI). This option, if selected, allows an operator to not login for downloading the SMS Client software (which is outside the module's cryptographic boundary) and SMS module documentation. The SMS Homepage still requires operator authentication in order to view and download module's reports and logs.

4.4 Secure Setup and Installation

The Crypto-Officer is responsible for successful and accurate first-time installation and initialization of the module upon delivery by following the below procedure:

a) The Crypto-Officer will receive the SMS firmware module version 3.2.0.8312 already installed in the test appliance from HP TippingPoint.
b) Upon reception of the appliance with the firmware module installed, the Crypto-Officer will place the appliance in a rack, if desired and connect the Ethernet port of the appliance to the network, and power port to a power outlet.
c) Then, access the module's console CLI using a directly attached monitor and a keyboard.
d) Power-on the appliance using the power button on the front side of the appliance.
e) After a successful start-up, the module will show a login prompt to the Crypto-Officer, where the username should be entered as "SuperUser" with no associated password. This would initiate the setup wizard, with the help of which, the Crypto-Officer will set the networking and management options for the module. The module always assumes the Crypto-Officer to perform the installation and thus, allows the Crypto-Officer services to this authenticated identity.
f) Now, using the console CLI, the Crypto-Officer must create operator accounts with usernames and corresponding passwords using the CLI command "users" and then by typing "A" for adding the username, "P" for entering the password corresponding to the newly created username, "R" for associating the newly added user with one of the available roles on the module and "E" for enabling this user account. The Crypto-Officer must create at least one Super-User Crypto-Officer account by following these steps, this login information for the Crypto-Officer will be used in the remaining steps.
g) The Crypto-Officer must then access the SMS Homepage (https://<IP address of the SMS module>) from another computer in the same subnet and login using the Super-User username and password established in the previous step and then download the SMS Client software from this webpage to the computer.
h) Then the Crypto-Officer will be required to start the SMS Client GUI on the same subnet computer and login using the Super-User Crypto-Officer login credentials.

The Crypto-Officer must then access Admin → General → 'SMS Patches' section → click 'Update'.

i) When the SMS Patch wizard opens up, select "Download from TMC" and click 'Next'. The GUI will then show the available patches on TMC which can be downloaded and imported into the module. Select the SMS Patch #3 file for this firmware version (SMS_Patch-3.2.0_8312.3.pkg) from the list. Click 'Download' and then click 'Install'.
j) The SMS module will now perform the necessary software load test on the patch file. If the patch file fails the self-test, the SMS Client GUI will show an error message and the incorrect patch file will be ignored and will not be installed into the module.
k) If the patch file passes the self-test, the SMS module will import the patch and will reboot automatically.
l) After the module reboots, if the SMS Client software will require an update for compatibility with the firmware version, a pop-up message will be shown and the Crypto-Officer must update the Client software for continuing access to perform module services.
m) The Crypto-Officer must ensure the current installed version in the SMS Client (Admin → General → SMS Patches) listed under 'Currently Installed' is 3.2.0.8312.3.
n) This procedure completes the initial setup configuration of the module. The Crypto-Officer should follow the procedure in section 4.1.1 for enabling FIPS-mode on the module.

4.5 Crypto-Officer Guidance

In order to maintain FIPS compliance of the module, the Crypto-Officer must follow the below guidance and rules:

- The Crypto-Officer must perform secure setup and installation of the module by following the instructions in Section 4.4.
  The Crypto-Officer must disable HTTP and Telnet using CLI commands "set svc.http-enable=no" and "set svc.telnet-enable=no". The Crypto-Officer must never enable HTTP and Telnet while the module operates in Full FIPS mode. The Crypto-Officer must ensure that the CLI commands "get svc.http-enable" and "get svc.telnet-enable" return "no". Alternatively, this can be ensured using the SMS Client GUI by accessing Admin → Server Properties → 'Services' section and making sure that HTTP and Telnet are always unchecked.
- The Crypto-Officer is required to maintain the BIOS password-locked and to not release the password information to any other operator while the module operates in FIPS-mode to avoid unauthorized access.
- Do not edit boot options in the BIOS for the test appliance used while the module is operating in Full FIPS mode.
- The Crypto-Officer must ensure that the 'password security level' for usernames and passwords is maintained at Level 1 or above at all times in FIPS-approved mode by accessing the CLI and executing the command "get pwd.level" or by using the SMS Client GUI and accessing Edit → Preferences → System → Password Preferences. Since the module allows only the Crypto-Officer to have

access to the CLI and to these specific Client options, no other users can edit this setting and the Crypto-Officer must never change the level to Level 0 while the module is running in Full FIPS mode.

- The Crypto-Officer must ensure that failed attempts threshold for locking out a user is always enabled and is configured at or above the value of 5 incorrect attempts, while the module is operating in the Full FIPS Mode. The module allows only the Super-User Crypto-Officer to access and modify this option. The Crypto-Officer must ensure this setting using the SMS Client GUI and accessing Edit → Preferences → System → Password Preferences.
- While using RADIUS or Active Directory server for remote authentication to the SMS module, a minimum of 8-character password and 8-character shared secret must be used.
- The Crypto-Officer must add users, configure their passwords and roles and enable the usernames as and when required.
- Follow the steps in the section 4.1 for enabling/disabling FIPS mode, generating/zeroizing keys, etc. to ensure the SMS operates in a FIPS-compliant manner.

4.6 User Guidance

In order to maintain FIPS compliance of the module, the User must follow the below guidance and rules:

- While using RADIUS or Active Directory server for remote authentication to the SMS module, a minimum of 8-character password and 8-character shared secret must be used.

4.7 Physical Security Rules

The TippingPoint SMS module was tested on the HP ProLiant DL320 G6 Server appliance which satisfies the requirements for FIPS 140-2 Level 1 Physical Security. The test platform uses production-grade enclosures and components. No other specific physical security mechanisms are required.

5 Security Relevant Data Items and Access Control

This section specifies the TippingPoint SMS Security Relevant Data Items (SRDIs) as well as the access control policy enforced by the SMS.

5.1 Cryptographic Algorithms

When in Full FIPS mode, the SMS uses only the cryptographic algorithms listed in Table 7 below.

Table 7: FIPS-Mode Cryptographic Algorithms

Algorithm Type/Name	Options	FIPS Certificate #
Asymmetric Algorithms		
RSA	1024-bit, 2048-bit modulus	#805, #806
DSA	1024 bit modulus	#513
Symmetric Algorithms		
AES	128, 192, 256 bit	#1631, #1632
Triple-DES	2-key and 3-key	#1067, #1068
Hashing Algorithms		
SHA	SHA-1, 224, 256, 384, 512	#1436, #1437
HMAC-SHA	SHA-1, 224, 256, 384, 512	#958, #959
Random Number Generators		
ANSI X9.31	AES-128, 192, 256 bit. Used wherever random numbers are required in SSH operations.	#874
SP800-90 DRBG	Hash DRBG using SHA-256. Used wherever random numbers are required in TLS operations.	#87
Key Agreement / Key Establishment Algorithms		
Diffie-Hellman Key Agreement (used with SSH and TLS)	Provides between 80 and 112 bits of encryption strength	Not FIPS-approved but allowed in FIPS mode.
RSA Key Transport (used with TLS)	Provides between 80 and 112 bits of encryption strength	Not FIPS-approved but allowed in FIPS mode.

The SMS supports the following non-FIPS approved cryptographic algorithms in the FIPS-approved ‘Full’ mode:

Table 8: Non-FIPS Mode Cryptographic Algorithms

Algorithm Type/Name	FIPS-approved
DES	No
RC2	No
RC4	No
RC5	No
SEED	No

CAMELLIA	No
MD2	No
MD5	No
CAST	No
IDEA	No
Blowfish	No

5.2 Cryptographic Keys, CSPs, and SRDIs

While operating in a FIPS-compliant manner, the TippingPoint SMS module contains the following security relevant data items:

Table 9: SRDI Information

Security Relevant Data Item	SRDI Description	Size or Modulus	Generation/ Entry	Storage	Output	Zeroization
RNG seed	Seed for the ANSI X9.31 RNG	128 bit	Not entered. Generated using an internal entropy data collection method.	Ephemeral: Plaintext in RAM	No	Zeroized on reboot or power cycle.
RNG seed key	AES seed key for the ANSI X9.31 RNG	128, 192 or 256 bit	Not entered. Generated using an internal entropy data collection method.	Ephemeral: Plaintext in RAM	No	Zeroized on reboot or power cycle.
Hash_DRBG Entropy	Entropy for Hash_DRBG	880 bit	Not entered. Generated using an internal entropy data collection method	Ephemeral: Plaintext in RAM	No	Zeroized on reboot or power cycle.
Hash_DRBG V value	Value of V for Hash_DRBG	440 bit	Not entered. Generated using an internal entropy	Ephemeral: Plaintext in RAM	No	Zeroized on reboot or power cycle.

			data collection method			
Hash_DRBG C value	Value of C for Hash_DRBG	440 bit	Not entered. Generated using an internal entropy data collection method	Ephemeral: Plaintext in RAM	No	Zeroized on reboot or power cycle.
Software/ Firmware load test key	PKCS#1 RSA public key used to verify all software updates to the module.	2048 bit	Not generated. Entered encrypted with TLS session key during software package install	Persistent: Stored in plaintext on hard drive.	No	A public key so no need to zeroize.
Password	Operator password	8-32 characters	Not generated. Entered by an operator encrypted with TLS or SSH session key or in plaintext (serial port or directly using a keyboard).	Persistent: Hashed using SHA256 and stored on hard drive.	No	Zeroized while entering or exiting the approved Full FIPS mode. Also overwritten with new passwords while changing passwords.
RADIUS Shared Secret	Shared secret used by the module to authenticate to the RADIUS server	Minimum 8 characters	Not generated. Entered by an operator encrypted with TLS using SMS Client	Persistent: Plaintext and stored on hard drive.	Output in plaintext to enable the module to authenticate to the RADIUS server	Zeroized while entering or exiting the approved Full FIPS mode.
Active Directory Shared Secret	Shared secret used by the module to authenticate to the Active Directory	Minimum 8 characters	Not generated. Entered by an operator encrypted with TLS	Persistent: Plaintext and stored on hard drive.	Output in plaintext to enable the module to authenticate to the	Zeroized while entering or exiting the approved Full FIPS

	server		using SMS Client		Active Directory server	mode.
Temporary TLS RSA key pair	RSA public/private keys used for TLS. This can only be used for importing the official key pair. No services are accessible over SMS Homepage and SMS Client using this key pair	1024 bits	Not entered. Generated by the module using the approved DRBG when FIPS mode is enabled.	Persistent: Plaintext and stored on hard drive.	Public key is output to its peer as part of TLS negotiation. Private key is never outputted.	Zeroized when new signed key pair is installed or when entering or exiting the approved Full FIPS mode.
Official TLS RSA key pair	Vendor-signed RSA public/private key pair used for TLS in FIPS-mode	2048 bits	Not generated. Imported by an operator over a TLS session using the temporary TLS RSA key pair.	Persistent: Plaintext and stored on hard drive.	Public key is output to its peer as part of TLS negotiation. Private key is never output.	Zeroized while entering or exiting the approved Full FIPS mode.
TLS Diffie-Hellman Key Pair	Diffie-Hellman public and private parameters	1024, 2048 bits	Not entered. Generated by the module using the approved DRBG	Ephemeral: Plaintext in RAM	No	Zeroized on reboot or power cycle.
TLS Pre-Master Secret	Shared secret exchanged using RSA Key Transport or established using Diffie-Hellman key exchange. This is used to derive the Master Secret	48 bytes if RSA key transport is used. 1024 or 2048 bits if Diffie-Hellman key exchange is used	May enter encrypted with the module's RSA public key or can be generated internally using DRBG or can be established	Ephemeral: Plaintext in RAM	May be outputted encrypted with the peer's RSA public key.	Zeroized on reboot or power cycle or when the ongoing TLS session ends.

			using Diffie-Hellman parameters.			
TLS master secret	Master Secret used to derive the encryption and MAC keys for both ends of an SSL session	48 Bytes	Not entered. Computed as part of SSL negotiation according to TLS 1.0 standard using the pre-master secret and nonces.	Ephemeral: Plaintext in RAM	No	Zeroized on reboot or power cycle or when the ongoing TLS session ends.
TLS encryption key	AES/Triple-DES symmetric key for SSL encryption in one direction	AES: 128, 192, or 256 Bits; Triple-DES: 112 or 168 Bits	Not entered. Derived from master secret as part of SSL negotiation.	Ephemeral: Plaintext in RAM	No	Zeroized on reboot or power cycle or when the ongoing TLS session ends.
TLS integrity key	MAC key for integrity in one direction	160 Bits	Not entered. Derived from master secret as part of SSL negotiation.	Ephemeral: Plaintext in RAM	No	Zeroized on reboot or power cycle or when the ongoing TLS session ends.
SSH Diffie-Hellman key pair	Public value and private exponent used for SSH DiffieHellman Key Exchange	1024, 2048 bits	Module's private exponent is generated during SSH negotiation using ANSI X9.31 RNG. The public value is derived from the private	Ephemeral: Plaintext in RAM	No	Zeroized on reboot or power cycle or when the ongoing SSH session ends.

			exponent and the Diffie-Hellman group. The peer's Diffie-Hellman public value enters the module according to SSH Standard.			
SSH RSA key pair	RSA public and private key pair	2048 Bits	Not entered. Generated using ANSI X9.31 RNG during key generation.	Persistent: Plaintext and stored on hard drive.	Public key is output to its peer as part of SSH negotiation. Private key is never outputted.	Zeroized while entering or exiting the approved Full FIPS mode.
SSH DSA key pair	DSA public and private key pair	1024 bits	Not entered. Generated using ANSI X9.31 RNG during key generation.	Persistent: Plaintext and stored on hard drive.	Public key is output to its peer as part of SSH negotiation. Private key is never outputted.	Zeroized while entering or exiting the approved Full FIPS mode.
SSH Diffie-Hellman shared secret	Shared secret used to derive client/server IVs, client/server encryption keys and client/server integrity keys for an SSH session	1024, 2048 bits	Not entered. Derived during SSH negotiation.	Ephemeral: Plaintext in RAM	No	Zeroized on reboot or power cycle or when the ongoing SSH session ends.
SSH session key	AES/Triple-DES symmetric key for SSH encryption in one direction	AES: 128, 192, or 256 Bits; Triple-DES: 112	Not entered. Derived during SSH negotiation.	Ephemeral: Plaintext in RAM	No	Zeroized on reboot or power cycle or when the ongoing

		or 168 Bits				SSH session ends.
SSH integrity key	MAC key for integrity in one direction	160 Bits	Not entered. Derived during SSH negotiation.	Ephemeral: Plaintext in RAM	No	Zeroized on reboot or power cycle or when the ongoing SSH session ends.

5.3 Access Control Policy

The SMS allows controlled access to the SRDIs contained within it. The following table defines the access that the SMS services have to the SRDIs (i.e. R=read, W=write, Z=zeroize, D=delete). If no access is listed, the service does not use that SRDI.

Table 10: Access Control Policy

Service / CSPs	**RNG seed and seed key**	**DRBG Entropy Input, C value, V value**	**Firmware load test key**	**Operator passwords**	**RADIUS and Active Directory Shared Secret**	**TLS RSA key pair**	**TLS DH pair, master secret, session key, integrity key**	**SSH RSA and DSA key pair**	**SSH DH pair, DH shared secret, session key, and integrity key**
Enable/disable Full FIPS mode	WZ	WZ		W Z	Z	WZ	RZ	WZ	RZ
View FIPS mode status							R		R
View self-test failure log file							R		
Configure own password				W			R		R
Configure any operator's password and access level				W			R		R
Add or delete users				D W			R		R

Configure ‘password security level’ and account lockout settings							R		R
Install new firmware or software patch	WZ	WZ	R W				RZ		Z
Import or download non-cryptography relevant software package							R		R
Activate or delete non-cryptography relevant software package							R		R
Reboot	WZ	WZ					RZ		RZ
Perform FIPS power-up self-tests									
Install new TLS RSA key pair						RW	R		
Login to CLI (console and SSH)	RW	RW		R	R			R	RW
Login to SMS Homepage	RW	RW		R	R	R	RW		
Login to SMS Client	RW	RW		R	R	R	RW		
Configure non-FIPS related admin level settings							R		R
Configure non-FIPS related super-user level settings							R		R
View non-FIPS related configuration							R		R
View non-FIPS related status							R		R

6 Mitigation of Other Attacks

The cryptographic module does not claim to mitigate any other attacks in a FIPS-approved mode of operation.