Symantec, A Division of Broadcom
Symantec Integrated Secure Gateway

Models: SSP-S410-10, SSP-S410-20, SSP-S410-30, SSP-S410-40, SSP-S210-10
SSP-S410 Hardware Versions: 090-20000-02, 090-20001-02, 090-20002-02, 090-20003-02
SSP-S210 Hardware Version: 090-20012-01
FIPS Security Kit Version: HW-KIT-FIPS-S410, HW-KIT-FIPS-S210
Firmware Version: 2.4.2.1

FIPS 140-2 Non-Proprietary Security Policy

FIPS 140-2 Security Level: 2
Document Version: 1.0

CONTACT INFORMATION

Symantec, A division of Broadcom
1320 Ridder Park Dr,
San Jose, CA 95131
www.broadcom.com

Table of Contents

List of Figures

List of Tables

1 Introduction

1.1 Purpose

This is a Non-Proprietary Cryptographic Module Security Policy for the Symantec Integrated Secure Gateway (ISG) appliances (Firmware Version 2.4.2.1; Models: SSP-S410-10, SSP-S410-20, SSP-S410-30, SSP-S410-40, S210-10) from Symantec, A division of Broadcom. This Non-Proprietary Security Policy describes how the ISG SSP-S410 and SSP-S210 meet the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S. and Canadian Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) and the Canadian Centre for Cyber Security (CCCS) Cryptographic Module Validation Program (CMVP) website at http://csrc.nist.gov/groups/STM/cmvp.

This document also describes how to run the appliance in the Approved mode of operation. This policy was prepared as part of the Level 2 validation of the module. The Symantec Integrated Secure Gateway is referred to in this document as ISG, crypto module, or module.

1.2 References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The Symantec website (www.broadcom.com) contains information on the full line of products from Symantec.
- The CMVP website (http://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search/) contains contact information for individuals to answer technical or sales-related questions for the module.

1.3 Document Organization

The *Non-Proprietary Security Policy* document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- *Vendor Evidence* document
- *Finite State Model* document
- *Entropy Assessment Report* document
- Other supporting documentation as additional references

With the exception of this *Non-Proprietary Security Policy*, the FIPS 140-2 Submission Package is proprietary to Symantec and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Symantec.

2 Symantec Integrated Secure Gateway

2.1 Integrated Secure Gateway Overview

The Symantec Integrated Secure Gateway (ISG) provides a flexible solution offering a new paradigm for solution deployment from traditional HW appliances. Compared to the previous HW appliances, this new hardware platform offers significant performance improvements, deployment flexibility, greater scalability and cost savings. It separates the hardware purchase from the software purchase, which enables the adoption of new enterprise licensing so customers can choose how they deploy the software – on-premises, as a virtual appliance, or in the cloud.

See Figure 1 below for a typical deployment scenario for ISG appliances.

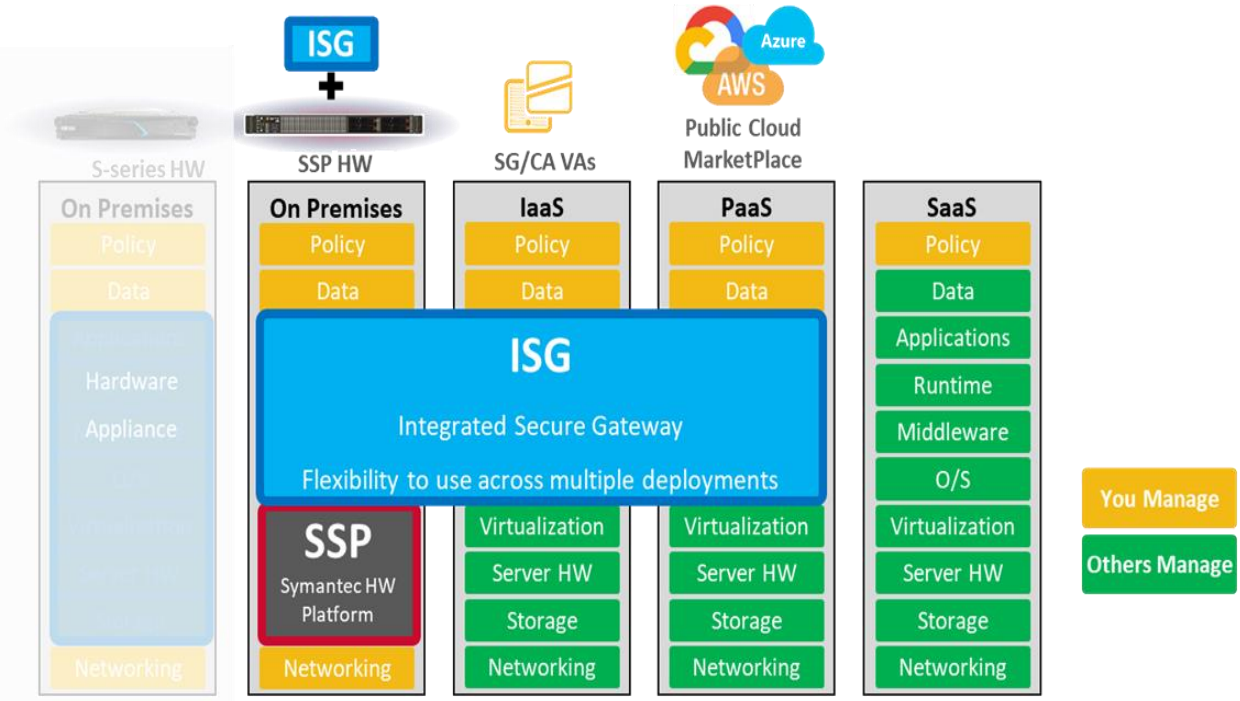

Figure 1 Typical Deployment of the S410 and S210 Modules

The Symantec Integrated Secure Gateway (ISG) software runs on the newest Symantec Security Platform SSP-S410 and S210 appliances. The ISG SSP-S210 and S410 appliances enable organizations to take a modular approach to network security by separating the traditional hardware-based appliance approach into individual software and hardware components. This allows customers to tailor their software and hardware procurement needs specifically to their network topology, providing on-premises, cloud-based, or blended solutions.
Additionally, the SSP appliances offer a significant performance improvement, keeping pace with the growing number of threats and volume of encrypted traffic where threats may be hidden. The new SSP S210 and S410 appliances offer the following benefits:

- Separation of Hardware and Software – This separation optimizes the customer's upgrade experience as hardware and software components may follow separate upgrade paths and enhancements can be adopted more quickly.

- Flexible licensing and portability – The new hardware supports the new enterprise licensing.
- Easier scalability – Add capacity as needed, where and when you need it.
- Significantly higher performance – The new hardware will deliver up to 5 Gbps of throughput with 90% of web traffic being SSL encrypted.
- Simplified configurations – From 43 hardware appliance models down to just four, without the need of upgrade kits.
- Hardware consolidation – Using Secure Web Gateway (SWG) hardware for comparison, customers can now achieve the same performance in 1U of rack space as they could in 8U of rack space using the previous highest performance option of the SWG hardware (note these appliances are also 2U) – up to an 8X performance per rack unit improvement.
- Reduce Data Center Costs – With reduced footprint, customers can reduce requirements for rack space, power, cooling and management.

With ISG, customers can easily transition from on-premises hardware (SSP appliances) to local virtualization (ESX/KVM) or public cloud (AWS, Azure, Google Cloud). The ISG SSP S210 and S410 appliances provide improved scalability by allowing capacity to be added, resized, aggregated, or split as needed.

ISG is validated at the following FIPS 140-2 Section levels in Table 1.

Table 1 Security Level per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	2
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	(N/A)
7	Cryptographic Key Management	2
8	Electromagnetic Interference/Electromagnetic Compatibility	2
9	Self-tests	2
10	Design Assurance	3
11	Mitigation of Other Attacks	N/A

2.2 Module Specification

For the FIPS 140-2 validation, the crypto module was tested on the following appliance configurations listed in Table 2.

Table 2 ISG Appliance Configuration

Appliance Type	Model/SKU	Hardware Version (part number)
SSP-S410	SSP-S410-10	090-20000-02
	SSP-S410-20	090-20001-02
	SSP-S410-30	090-20002-02
	SSP-S410-40	090-20003-02
SSP-S210	SSP-S210-10	090-20012-01

The hardware version numbers in Table 2 represent different performance options available for the S410 and the S210. The appliance models differ in the processor (model and count), disk storage, and memory. All appliance models run the same firmware version and are the same from a cryptographic functionality and boundary perspective.

For the FIPS 140-2 validation, the ISG module was tested on the following appliance configurations:

- SSP-S410-10, SSP-S410-20, SSP-S410-30, SSP-S410-40, SSP-S210-10 running firmware version 2.4.2.1.

Symantec ISG is a module with a Multi-chip Standalone embodiment. The overall security level of the module is 2. The cryptographic boundary is defined by the appliance chassis, shown in Figure 2 below, which surrounds all the hardware and firmware.

Figure 2 Physical Boundary

The module firmware, version 2.4.2.1, contains the following cryptographic libraries:

- ISG Cryptographic Library v1.0
- ISG UEFI OS Loader Library v4.26
- ISG LRNG Library v1.0

2.3 Module Interfaces

The module's physical ports can be categorized into the following logical interfaces defined by FIPS 140-2:

- Data input
- Data output
- Control input
- Status output

The S410 and the S210 front panel each have five Light Emitting Diodes (LEDs), two control buttons, and two USB ports. The front panel control buttons are disabled once the module is configured for its Approved mode of operation. The USB ports provide no user functionality. The front panel of the S410 is shown in Figure 3.

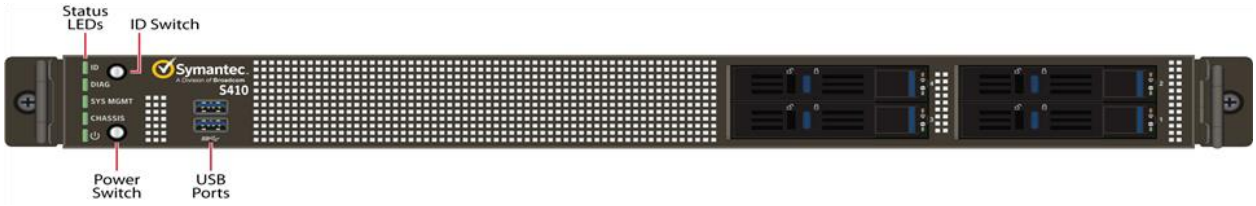

Figure 3 Front Panel of the S410

See the front panel of the S210 below in Figure 4.

Figure 4 Front Panel of the S210

The type and quantity of all ports on the S410 and S210 front panels are shown in Table 3.

Table 3 FIPS 140-2 Logical Interface Mappings on the S410 and the S210 Front Panel

Physical Port / Interface	Quantity	FIPS 140-2 Interface
LEDs	5	Status Output
Power Button	1	Power
ID Switch Button	1	N/A (port is inaccessible with physical security baffle installed)
USB Ports	2	N/A(port is disabled)

The status indications provided by the LEDs on the S410 and S210 front panel are described in Table 4.

Table 4 LED Status Indications on S410 and S210 Front Panel

LEDs	Color	Definition
ID	Off	Location off.
	Blinks blue	Lights up, when triggered by the appliance software, to help locate the appliance when it is rack-mounted.
Diagnosis	Off	No functionality enabled.
System Management	Off	No power is present or the appliance has been powered off.
	Green	Operating normally.

LEDs	Color	Definition
	Amber	The appliance has not yet been licensed or has encountered a system fault, indicating overheating, fan or battery failure, or other sensor failure.
	Blinks amber	The appliance has encountered a critical fault.
Chassis	Off	No intrusion detected.
	Amber	Intrusion detected.
Power	Off	No power is present or the appliance has been powered off.
	Green	The appliance is powered on and fully configured.
	Amber	The appliance is powered on and is in the process of booting.
	Blinks green to amber	The appliance is powered on but has not yet been initialized.

The S410 and the S210 have the same number of ports and interfaces on the front; however, the rear ports and interfaces differ between the S410-based models and the S210-based model. The rear of the S410-based models is shown in Figure 4 and the rear of the S210 based models is shown in Figure 6.

The rear of the S410, as shown in Figure 5, contains the following ports:

- Two Power Supply Unit (PSU) connectors
- A Console Port to connect to a Personal Computer (PC) for management
- One 4 port Gigabit 10/100/1000 Base T) Ethernet adapter
- One onboard 10/100/1000 Base T Ethernet adapter port for system management
- PCIe slots 1-4 (not a FIPS interface)

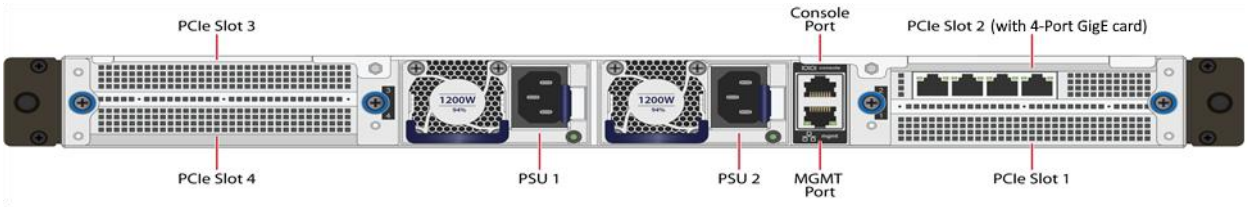

Figure 5 Rear Panel of the S410

The rear of the S210, as shown in Figure 6, contains the following ports:

- Two PSU connectors
- One console port to connect to a PC for management
- One USB port (disabled)
- Two GigE ports for system management
- Four GigEE ports
- PCIe slots 1-2 (not a FIPS interface)

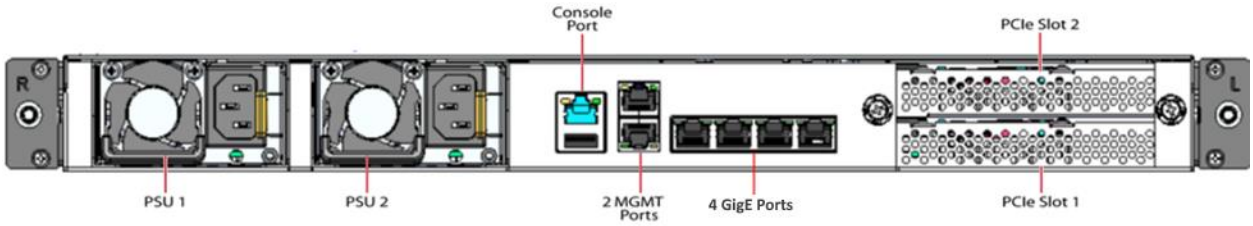

Figure 6 Rear Panel of the S210

The type and quantity of ports on the S410 and S210 rear panel are shown in Table 5.

Table 5 FIPS 140-2 Logical Interface Mappings on the S410 and S210 Rear Panel

Physical Port / Interface	Quantity	FIPS 140-2 Interface
GigE Ports	5 (S410) 6(S210)	■ Data Input ■ Data Output ■ Control Input ■ Status Output
System Management Port (MGMT Port)	1 (S410) 2 (S210)	■ Data Input ■ Data Output ■ Control Input ■ Status Output
Console (Serial) Port	1	■ Control Input ■ Status Output
Ethernet Interface – Speed LEDs	5 (S410) 6 (S210)	■ Status Output
Ethernet Interface – Activity LEDs	5 (S410) 6 (S210)	■ Status Output
PSU Connectors	2	■ Power Input

The status indications provided by the LEDs on the S410 and S210 rear panel are described in Table 6.

Table 6 LED Status Indications on S410 and S210 Rear Panel

LED	Color	Definition
AC power connection LED	Off	The module is not receiving power.
	Green	The module is receiving power.
	Blinks green	The module is receiving power but is in standby mode.
	Red	The module has encountered a fault or error.
Ethernet Interface – Activity LEDs	Off	No link is present.
	Green	Link is present

LED	Color	Definition
	Flashing green	Link activity.
Ethernet Interface – Speed Indicator LEDs	Amber	10 Mbps speed connection is present.
	Amber	100 Mbps speed connection is present.
	Green	1000 Mbps speed connection is present.

2.4 Roles and Services

Before accessing the modules for any administrative services, COs and Users must authenticate to the module according to the methods specified in Table 10. The modules offer the following management interface:

- CLI[1] – This interface is used for management of the modules. This interface must be accessed locally via the serial port to perform the initial module configurations (IP address, DNS server, gateway, and subnet mask) and placing the modules into the Approved mode. When the module has been properly configured, this interface can be accessed via SSH[2]. Management of the module may take place via SSH or locally via the serial port. Authentication is required before any functionality will be available through the CLI.

When managing the module over the CLI, COs and Users both log into the module with accounts entering the "standard", or "unprivileged" mode on the CLI. Unlike Users, COs have the ability to enter the "enabled" or "privileged" mode after initial authentication to the CLI by supplying the "enabled" mode password. Additionally, COs can only enter the "configuration" mode from the "enabled" mode via the CLI, which grants privileges to make configuration level changes. Going from the "enabled" mode to the "configuration" mode does not require additional credentials. The details of these modes of operation are found below in Table 10.

The CO and User details are found below in Table 7.

Table 7 FIPS and ISG Roles

FIPS Roles	Module Roles and Privileges
CO	The CO is an administrator of the module that has been granted "enabled" mode access while using the CLI. When the CO is using the CLI, and while in the "enabled" mode of operation, COs may put the module in its Approved mode, reset to the factory state, and query if the module is in the Approved mode. In addition, COs may do all the services available to Users while not in the "enabled" mode. Once the CO has entered the "enabled" mode, the CO may then enter the "configuration" mode via the CLI. The "configuration" mode provides the CO management capabilities to perform tasks such as account management and key management.
User	The User is an administrator of the module that operates only in the "standard" or "unprivileged" mode and has not been granted access to the "enabled" mode in the CLI.

Descriptions of the services available to a Crypto Officer (CO) and User are described below in Table 8 respectively. For each service listed below, COs and Users are assumed to already have authenticated prior to attempting to

[1] CLI – Command Line Interface
[2] SSH – Secure Shell protocol

execute the service. There are no additional services that are unauthenticated. Please note that the keys and CSPs listed in the table indicate the type of access required using the following notation:

- **R**: The CSP is read
- **W**: The CSP is established, generated, modified, or zeroized
- **X:** Execute: The CSP is used within an Approved or Allowed security function or authentication mechanism.

2.4.1 Crypto-Officer Role

Descriptions of the FIPS 140-2 relevant services available to the Crypto-Officer role are provided in Table 8 below. Additional services that do not access CSPs can be found in the *Symantec Integrated Secure Gateway Command Line Overview, v2.4* located here:

https://techdocs.broadcom.com/us/en/symantec-security-software/web-and-network-security/integrated-secure-gateway/2-4/cli_Command-Line-Overview.html

Table 8 Crypto Officer Role Services and CSP Access

Service	Description	CSP and Access Required
Set up the module (serial port only)	Set up the first-time network configuration, CO username and password, and enable the module in the Approved mode of operation. For more information, see section 3.3.1 in this *Security Policy*.	CO Password: W “Enabled” mode password: W
Enter the “enabled” mode	Manage the module in the “enabled” mode of operation, granting access to higher privileged commands	“Enabled” mode password: RX
* Enter the “configure” mode	Manage the module in the “configuration” mode of operation, allowing permanent system modifications to be made	None
* Disable FIPS mode	Take the module out of the approved mode of operation and restore it to a factory state	SSH Session Key: W SSH Integrity Key: W TLS Session Key: W TLS Integrity Key: W TLS Pre-Master Secret: W TLS Master Secret: W KAS-FFC private key: W KAS-ECC private key: W DRBG CSPs: W DPK: W CO Password: W User Password: W “Enabled” mode password: W RSA Private Key: W
Syslog over TLS	Configure the module to use syslog via TLS	RSA public key: RX RSA private key: RX

Service	Description	CSP and Access Required
		KAS-FFC public key: WRX KAS-FFC private key: WRX KAS-ECC public key: WRX KAS-ECC private key: WRX TLS Session Key: W TLS Integrity Key: W TLS Pre-Master Secret: W TLS Master Secret: W DRBG CSPs: WRX
** Firmware Load	Loads new external firmware and performs an integrity test using an RSA digital signature using the "installed-systems load" command.	Integrity Test public key: WRX
Create remote management session	Manage the module through the CLI (SSH) remotely via Ethernet port.	RSA public key: RX RSA private key: RX KAS-FFC public key: WRX KAS-FFC private key: WRX KAS-ECC public key: WRX KAS-ECC private key: WRX SSH Session Key: WRX SSH Integrity Key: WRX DRBG CSPs: WRX DPK: RX CO Password: R
** Create, edit, and delete User Groups	Create, edit and delete operator groups; define common sets of operator permissions.	None
**Create, edit, and delete operators	Create, edit and delete operators (these may be COs or Users); define operator's accounts, change password, and assign permissions.	Crypto-Officer Password: W User Password: W DPK: RX
Show FIPS-mode status	The CO logs in to the module using the CLI. Entering the command "show version" will display if the module is configured in Approved mode.	None
* Zeroize keys	Zeroize keys by taking the module out of the Approved mode and restoring it to a factory state. This will zeroize all CSPs. The zeroization occurs while the module is still in Approved-mode.	SSH Session Key: W SSH Integrity Key: W TLS Session Key: W TLS Integrity Key: W TLS Pre-Master Secret: W TLS Master Secret: W KAS-FFC private key: W KAS-ECC private key: W DPK: W CO Password: W User Password: W "Enabled" mode password: W RSA Private Key: W

Service	Description	CSP and Access Required
Query deployed applications and application resources	View information and statistics on the deployed applications on the module	None
Configure and query password policy	Configure and view the current password policy employed by the module.	None
** Change password	Change Crypto-Officer password	Crypto-Officer Password: RW DPK: RX
* Perform self-test	Perform self-test on demand by rebooting the machine	KAS-FFC public key: W KAS-FFC private key: W KAS-ECC public key: W KAS-ECC private key: W SSH Session Key: W SSH Integrity Key: W TLS Session Key: W TLS Integrity Key: W TLS Pre-Master Secret: W TLS Master Secret: W DRBG CSPs: W

* - Indicates services that are only available once the CO has entered the “enabled” mode of operation.
** - Indicates services that are only available once the CO has entered the “enabled” mode followed by the “configuration” mode of operation.

2.4.2 User Role

Descriptions of the FIPS 140-2 relevant services available to the User role are provided in Table 9 below. Additional services are that do not access CSPs can be found in the *Symantec Integrated Secure Gateway Command Line Overview, Version 2.4:*

https://techdocs.broadcom.com/us/en/symantec-security-software/web-and-network-security/integrated-secure-gateway/2-4/cli_Command-Line-Overview.html

Table 9 User Service and CSP Access

Service	Description	CSP and Access Required
Create remote management session	Manage the ISG Module using the CLI (SSH) remotely via Ethernet port.	RSA public key: RX RSA private key: RX Client RSA public key: RX KAS-FFC public key: RX KAS-FFC private key: RX KAS-ECC public key: RX KAS-ECC private key: RX SSH Session Key: WRX SSH Integrity Key: WRX DRBG CSPs: WRX DPK: RX
Show FIPS-mode status	Entering the command “show version” will display if the module is configured in Approved Mode.	None

Service	Description	CSP and Access Required
Show deployed applications and application resources	View information and statistics on the deployed applications on the module using the "show applications" command.	None
Show password policy	View the current password policy employed by the module using the "show password-policy-configuration" command.	None
Change password	Change User password	User Password: RW DPK: RX

2.4.3 Authentication Mechanism

The module supports role-based authentication. COs and Users must authenticate using a private key (user ID and password), or can alternatively use RSA public key authentication for SSH to set up the secure session. Secure sessions that authenticate Users have no interface available to access other services (such as Crypto Officer services). Each CO or User SSH session remains active (logged in) and secured until the operator logs out or inactivity for a configurable amount of time has elapsed.

The authentication mechanisms used in the module are listed in Table 10.

Table 10 Authentication Mechanisms Used by Module

Role	Authentication Type	Authentication Strength
Crypto-Officer	Password	The modules support password authentication internally. For password authentication done by the modules, passwords are required to be at minimum 8 characters in length, and at maximum 64 bytes (number of characters is dependent on the character set used by system). An 8-character password allowing all printable American Standard Code for Information Interchange (ASCII) characters (95) with repetition equates to a 1:(95^8), or 1:6,634,204,312,890,625 chance of false acceptance. The Crypto-Officer may connect locally using the serial port or remotely after establishing a TLS or SSH session. The fastest network connection supported by the module is 1000 Mbps. Hence at most (1000 ×10^6 × 60 = 6 × 10^10 =) 60,000,000,000 bits of data can be transmitted in one minute. Therefore, the probability that a random attempt will succeed or a false acceptance will occur in one minute is: 1 : [95^8 possible passwords / ((6 ×10^10 bits per minute) / 64 bits per password)] 1: (95^8 possible passwords / 937,500,000 passwords per minute) This equals 1: 7,076,484 or approximately 1 in 7.0 million; this is less than 1:100,000 as required by FIPS 140-2.
	Password ("Enabled" Mode)	The modules support password authentication internally. For password authentication done by the modules, passwords are required to be at least 8 characters in length and maximum of 64 bytes (number of characters is dependent on the character set used by system). An 8-character password allowing all printable American Standard Code for Information Interchange

Role	Authentication Type	Authentication Strength
		(ASCII) characters (95) with repetition equates to a 1: (95^8), or 1:6,634,204,312,890,625 chance of false acceptance. This password is entered by the Crypto-Officer to enter the "enabled" mode; this is entered locally through the serial port or remotely after establishing an SSH session. The fastest network connection supported by the module is 1000 Mbps. Hence at most (1000 ×10^6 × 60 = 6 × 10^10 =) 60,000,000,000 bits of data can be transmitted in one minute. Therefore, the probability that a random attempt will succeed or a false acceptance will occur in one minute is: 1 : [95^8 possible passwords / ((6 ×10^10 bits per minute) / 64 bits per password)] 1: (95^8 possible passwords / 937,500,000 passwords per minute) This equals 1: 7,076,484 or approximately 1 in 7.0 million; this is less than 1:100,000 as required by FIPS 140-2.
	SSH RSA Client keys	The module supports using SSH RSA client keys for authentication of COs during SSH. Using conservative estimates and equating a 2048-bit RSA key to a 112-bit symmetric key, the probability for a random attempt to succeed is $1:2^{112}$ or 1: 5.19 x 10^{33}. The fastest network connection supported by the module is 1000 Mbps. Hence at most (1000 ×10^6 × 60 = 6 × 10^10 =) 60,000,000,000 bits of data can be transmitted in one minute. Therefore, the probability that a random attempt will succeed or a false acceptance will occur in one minute is less than 1: (2^112 / 6×10^10), or 1: 86,538,280,975,580,460,475,508, which is less than 1:100,000 as required by FIPS 140-2.
User	Password	The modules support password authentication internally. For password authentication done by the modules, passwords are required to be at least 8 characters in length and maximum of 64 bytes (number of characters is dependent on the character set used by system). An 8-character password allowing all printable American Standard Code for Information Interchange (ASCII) characters (95) with repetition equates to a 1:(95^8), or 1: 6,634,204,312,890,625 chance of false acceptance. The User may connect remotely after establishing a TLS or SSH session. The fastest network connection supported by the module is 1000 Mbps. Hence at most (1000 ×10^6 × 60 = 6 × 10^10 =) 60,000,000,000 bits of data can be transmitted in one minute. Therefore, the probability that a random attempt will succeed or a false acceptance will occur in one minute is: 1 : [95^8 possible passwords / ((6 ×10^10 bits per minute) / 64 bits per password)] 1: (95^8 possible passwords / 937,500,000 passwords per minute) This equals 1: 7,076,484 or approximately 1 in 7.0 million; this is less than 1:100,000 as required by FIPS 140-2.
	SSH RSA Client keys	The module supports using SSH RSA client keys for authentication of Users during SSH. Using conservative estimates and equating a 2048-bit RSA key to a 112-bit symmetric key, the probability for a random attempt to succeed is $1:2^{112}$ or 1: 5.19 x 10^{33}. The fastest network connection supported by the module is 1000 Mbps. Hence at most (1000 ×10^6 × 60 = 6 × 10^10 =) 60,000,000,000 bits of data can

Role	Authentication Type	Authentication Strength
		be transmitted in one minute. Therefore, the probability that a random attempt will succeed or a false acceptance will occur in one minute is less than 1: (2^112 / 6×10^10), or 1: 86,538,280,975,580,460,475,508, which is less than 1:100,000 as required by FIPS 140-2.

2.5 Physical Security

The ISG is a Multi-Chip Standalone cryptographic module. It is enclosed in a hard, opaque metal case that completely encloses all its internal components. There are only a limited set of vent holes provided in the case, and these holes obscure the view of the internal components of the module. The large hole on the front baffle will allow the power button to be accessed and no other buttons. Tamper-evident labels are applied to the case to provide physical evidence of attempts to remove the case of the module. The Crypto-Officer is responsible for the placement of tamper-evident labels and baffles, and guidance and instructions can be found in section 3. The labels and baffles are part of the FIPS Security Kit for the S410 (Part Numbers: 090-20000-02, 090-20001-02, 090-20002-02, 090-20003-02; HW-KIT-FIPS-S410) and for the S210 (Part Number 090-20012-01; HW-KIT-FIPS-S210) models.

All the module's components are production grade. The modules were tested and found conformant to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (i.e., for business use).

2.6 Non-Modifiable Operational Environment

The operational environment requirements do not apply to the modules. The module does not provide a general-purpose operating system. The operating system is not modifiable by the operator, and only the modules' signed image can be executed. All firmware upgrades are digitally signed, and a conditional self-test (RSA 2048 signature verification) is performed during each upgrade.

NOTE: Only FIPS-validated firmware may be loaded to maintain the module's validation.

2.7 Cryptographic Key Management

The module implements the FIPS-Approved algorithms listed below in Table 11, Table 12, and Table 13.

Note: There are algorithms, modes, and keys that have been CAVP tested but not used by the module. Only the algorithms, modes/methods, and key lengths/curves/moduli shown in this table are used by the module.

Table 11 FIPS-Approved Algorithm Implementations for the ISG Cryptographic Library v1.0

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli	Use
A1464	AES	SP 800-38A, FIPS 197	CBC, CTR, GCM[3]	AES 128, 256 CBC AES 128, 192, 256 CTR AES 128, 192[4], 256 GCM	Data Encryption / Decryption
A1464	KTS[5]	SP 800-38F	AES (CBC, CTR, GCM) and HMAC	AES 128, 256 CBC AES 128, 192, 256 CTR AES 128, 192[6], 256 GCM	Key Transport
A1464	AES	SP 800-38E	XTS	128, 256	Data Encryption / Decryption At Rest
A1464	SHS	FIPS 180-4	SHA-1, SHA-256, SHA-384, SHA-512		Message Digest

[3] AES GCM IV generation method complies with technique #2 in section A.5 of the Implementation Guidance for FIPS PUB 140-2. The AES GCM IV is used in the TLS protocol and in the SSH protocol. In all cases, the AES GCM IV is internally generated via RBG-based construction in compliance with Section 8.2.1 of NIST SP 800-38D using the Approved DRBG within the module's physical boundary and is at least 96 bits in length

[4] 192 GCM – While this key size was algorithm tested, it is not callable by the module.

[5] KTS - Key establishment methodology provides between 128 and 256 bits of encryption strength

[6] 192 GCM – While this key size was algorithm tested, it is not callable by the module.

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli	Use
A1464	HMAC	FIPS 198-1	HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	128, 256, 384, 512	Message Authentication
A1464	RSA	FIPS 186-4	SHA-256, SHA-384 PKCS1 v1.5	2048, 3072	Digital Signature Generation, Digital Signature Verification
A1464	RSA	FIPS 186-4	PKCS1 v1.5	2048	Keypair Generation
A1464	KTS-RSA[7]	SP800-56B rev 2	KTS-IFC (RSA-OAEP Basic)	2048	Key Transport
A1464	CTR-DRBG	SP 800-90A	CTR-based	AES-256	Deterministic Random Bit Generation
Vendor Affirmed	CKG	SP 800-133			Key Generation
A1464	KAS-SSC	SP 800-56A rev 3	FFC	(2048, 256)	Key Agreement Scheme – Key Agreement Scheme Shared Secret Computation (KAS-SSC) per SP 800-56Arev3, Key Derivation per SP 800-135rev1 (TLS KDF CVL. Cert. A1464 and SSH KDF CVL Cert. A1464).

[7] KTS-RSA - key establishment methodology provides 112 bits of encryption strength

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli	Use
A1464	KAS-SSC	SP 800-56A rev 3	ECC	P-256, P-384, P-521	Key Agreement Scheme – Key Agreement Scheme Shared Secret Computation (KAS-SSC) per SP 800-56Arev3, Key Derivation per SP 800-135rev1 (TLS KDF CVL. Cert. A1464 and SSH KDF CVL Cert. A1464).
A1464	CVL TLS 1.1, TLS 1.2	SP 800-135rev1	TLS 1.2 SHA Sizes = SHA-256, SHA384		Key Derivation
A1464	CVL SSH	SP 800-135rev1	AES-128 CBC, AES-256 CBC	SHA-1, SHA-256, SHA-512	Key Derivation

FIPS-Approved Algorithm Implementations for the three libraries are in Table 12 and Table 13 below.

Table 12 FIPS-Approved Algorithm Implementations for UEFI OS Loader Library v4.26

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli	Use
A1250	SHS	FIPS 180-4	SHA-1[8], SHA-256		Message Digest as part of Integrity Check
A1250	RSA	FIPS 186-4	SHA-256; PKCS1 v1.5	2048	Digital Signature Verification as part of Integrity Check
A1250	HMAC	FIPS 198-1	HMAC-SHA-1	128	Integrity Check

[8] SHA-1 is as part of HMAC-SHA-1 and is only used for verification purposes as part of the module integrity check.

Table 13 FIPS-Approved Algorithm Implementations for ISG LRNG Library v1.0

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli	Use
A1463	SHS	FIPS 180-4	SHA-512		Vetted conditioning component
A1463	CTR-DRBG	SP 800-90A	CTR-based	AES-256	Vetted conditioning component
A1463	AES	SP 800 38A	ECB	256	Vetted Conditioning component
-	ENT (NP[9])	SP 800-90B			Entropy Generation

Table 14 FIPS-Allowed Algorithms

Algorithm	Caveat	Use
RSA Signature Verification	1536, 2048	Signature Verification
MD5	No security is provided by this algorithm.	In TLS 1.1 Protocol

NOTE: No parts of the TLS or SSH protocols, other than the KDF, have been reviewed or tested by the CAVP and CMVP. FIPS-Allowed algorithms are listed above in Table 14.

The module supports the CSPs listed below in Table 15 below.

[9] NP - Non-Physical

Table 15 List of Cryptographic Key Components, and CSPs

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
Data Protection Key (DPK)	AES XTS 256-bit key	Internally generated via FIPS-Approved DRBG (per IG A.9)	Never exits the module	Stored in plaintext on non-volatile memory	By disabling the FIPS-Approved mode of operation	Encrypting Crypto-Officer password, User password, "Enabled" mode password, and RSA private key
Firmware Load Test Public Key	RSA public key 2048 bits	Externally generated, Imported in encrypted form via a secure SSH session	Never exits the module	Stored in plaintext on non-volatile memory	Overwritten after upgrade by the key in the newly signed image	Verifying the integrity of the system image during upgrade or downgrade
RSA Public Keys	2048-, 3072-, and 4096-bits	Modules' public key is internally generated via FIPS-Approved DRBG	Output during TLS/SSH[10] negotiation in plaintext.	Stored in encrypted form on non-volatile memory	Module's public key is deleted by command	Negotiating TLS or SSH sessions
SSH RSA Client key	2048, 3072, and 4096-bits	Other entities' public keys are sent to the module in plaintext	Never exits the module	Other entities' public keys reside on	Other entities' public keys are cleared by power cycle	Authentication for SSH sessions.
RSA Private Keys	2048-, 3072-, and 4096-bits	Internally generated via FIPS-Approved DRBG	Never exits the module	Stored in encrypted form on non-	Inaccessible by zeroizing encrypting DPK	Negotiating TLS or SSH sessions

[10] SSH session negotiation can only use RSA key pairs of 2048-bits. TLS session negotiation can use RSA key pairs of 2048-bits, 3072-bits and 4096-bits .

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
		Imported in encrypted form via a secure TLS or SSH session Imported in plaintext via a directly attached cable to the serial port		volatile memory		
KAS-FFC public key	2048-bits	Module's public key is internally generated via FIPS-Approved DRBG Public key of a peer enters the module in plaintext	The module's Public key exits the module in plaintext	Stored in plaintext on volatile memory	Rebooting the modules Removing power	Negotiating TLS or SSH sessions
KAS-FFC private key	224-bits	Internally generated via FIPS-Approved DRBG	Never exits the module	Stored in plaintext on volatile memory	Rebooting the modules Removing power	Negotiating TLS or SSH sessions
KAS-ECC private key	P-256 key[11]	Internally generated via FIPS-Approved DRBG	Never exits the module	Stored in plaintext on volatile memory	Rebooting the modules Removing power	Negotiating TLS or SSH sessions
KAS-ECC public key	P-256 key[12]	Module's public key is internally generated via FIPS-Approved DRBG	The module's Public key exits the module in plaintext	Stored in plaintext on volatile memory	Rebooting the modules	Negotiating TLS or SSH sessions

[11] While the P-256, P-384, and P-521 curves were tested, only P-256 can be called by the module in the Approved mode.

[12] While the P-256, P-384, and P-521 curves were tested, only P-256 can be called by the module in the Approved mode.

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
		Public key of a peer enters the module in plaintext			Removing power	
TLS Pre-Master Secret	384-bit key	Input in encrypted form from TLS client	Never	Stored in plaintext on volatile memory	Rebooting the modules Removing power	Establishing the TLS Master Secret
TLS Master Secret	384-bit key	Generated internally during session negotiation	Never exits the module	Stored in plaintext on volatile memory	Rebooting the modules Removing power	Establishing the TLS Session Key
TLS Session key	AES CBC 128-,or 256-bit key, AES GCM 128 or 256-bit key	Internally generated via FIPS-Approved DRBG	Output in encrypted form during TLS protocol handshake	Stored in plaintext on volatile memory	Rebooting the modules Removing power	Encrypting TLS data
SSH Session Key	AES CBC 128 or 256-bit key, AES CTR 128, 192, or 256-bit key, AES GCM 128 or 256-bit key	Internally generated via FIPS-Approved DRBG	Output in encrypted form during SSH protocol handshake	Stored in plaintext on volatile memory	Rebooting the modules Removing power	Encrypting SSH data
TLS Integrity key	HMAC SHA-1-, 256-bit, 384-bit key	Internally generated	Never exits the module	Resides in volatile memory in plaintext	Rebooting the modules Removing power	Data authentication for TLS sessions
SSH Integrity key	HMAC SHA-1-, 256-, 512-bit key	Internally generated	Never exits the module	Resides in volatile memory in plaintext	Rebooting the modules Removing power	Data authentication for SSH sessions
Crypto Officer Password	Minimum of eight (8) and maximum of 64	Externally generated. Enters the module in encrypted form via a	Exits in encrypted form via a secure TLS session	Stored in encrypted form on non-	Inaccessible by zeroizing the encrypted DPK	Locally authenticating a CO or User for

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
User Password	bytes long printable character string	secure TLS or SSH session. Enters the module in plaintext via a directly attached cable to the serial port	for external authentication	volatile memory		Management Console or CLI
"Enabled" mode password	Minimum of eight (8) and maximum of 64 bytes long printable character string	Enters the module in encrypted form via a secure SSH session Enters the module in plaintext via a directly attached cable to the serial port	Exits in encrypted form via a secure TLS session for external authentication	Stored in encrypted form on non-volatile memory	Inaccessible by zeroizing the encrypting DPK	Used by the CO to enter the "privileged" or "enabled" mode when using the CLI
SP 800-90A CTR_DRBG Seed[13]	384-bit random number	Internally generated	Never exits the module	Plaintext in volatile memory	Rebooting the modules Removing Power	Seeding material for the SP800-90A CTR_DRBG
SP 800-90A CTR_DRBG Entropy[14]	256-bit random number with derivation function	Internally generated	Never exits the module	Plaintext in volatile memory	Rebooting the modules Removing Power	Entropy material for the SP800-90A CTR_DRBG
SP 800-90A CTR_DRBG key value	Internal state value	Internally generated	Never	Plaintext in volatile memory	Rebooting the modules Removing Power	Used for the SP 800-90A CTR_DRBG

[13] The CTR DRBG Seed requires a 384-bit number and uses 256 bits of entropy with the derivation function to create the 384-bit value. The 256-bits of CTR DRBG Entropy is obtained from an entropy-generating ENT (NP) inside the module's cryptographic boundary

[14] The CTR DRBG Entropy required by the FIPS-Approved SP 800-90A CTR_DRBG (with AES-256) is supplied by the ENT (NP). The ENT(NP) provides a full 256 bits of entropy per IG 7.14 Scenario 1A.

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
SP 800-90A CTR_DRBG V value	Internal state value	Internally generated	Never exits the module	Plaintext in volatile memory	Rebooting the modules Removing power	Used for the SP 800-90A CTR_DRBG

NOTE: The Approved DRBG is seeded with a minimum of 384-bits from an entropy-generating ENT(NP) inside the module's cryptographic boundary.

2.8 Self-Tests

If the module fails the POST Integrity Test, the following error is printed to the CLI (when being accessed via the serial port):

```
Boot system failed signature verification
```

If a self-test fails in the ISG Cryptographic Library, the following error is printed to the CLI (when being accessed via the serial port):

```
Open ssl FIPS POST Test failed. Rebooting…
```

When these errors occur, the modules halt operation and provide no functionality. The only way to clear the error and resume normal operation is for the Crypto-Officer to reboot the modules. The status output provided below is shown only over the CLI (when being accessed via the serial port).

The sections below describe the self-tests performed by the module.

2.8.1 Power-Up Self-Tests

The module performs the following self-tests using the UEFI OS Loader Library:

- Known Answer Tests
  - HMAC KAT using SHA-1; and
  - RSA Sign/Verify KAT with SHA-256
- Firmware integrity check using HMAC-SHA-1

The module performs the following self-tests using the ISG LRNG Library:

- Known Answer Tests
  - SHA-512
  - AES ECB KAT for encryption and decryption
  - SP800-90A DRBG KAT

The module then performs the following self-tests using the ISG Cryptographic Library at power-up:

- Known Answer Tests
  - AES ECB 128 KAT for encryption and decryption
  - AES GCM 256 KAT for encryption and decryption
  - AES XTS 128/256 KAT for encryption and decryption
  - HMAC KAT using SHA-1, SHA-256, SHA-384, SHA-512
  - RSA Sign/Verify KAT with SHA-256
  - SP800-90A DRBG KAT
  - KAS-FFC-SSC KAT
  - KAS-ECC-SSC KAT

No data output occurs via the data output interface until all power-up self-tests have completed.

2.8.2 Conditional Self-Tests

The module performs the conditional self-tests for its ISG Cryptographic Library.

- RSA pairwise consistency check upon generation of an RSA keypair
- Continuous RNG test (CRNGT) for the SP800-90A DRBG
- CRNGT for the ENT (NP)
- Firmware Load Test using RSA Signature Verification

The module performs the conditional self-tests for its LRNG Cryptographic Library.

- The LRNG implements the Repetition Count Test (RCT) specified in SP800-90B section 4.4.1
- The LRNG implements the Adaptive Proportion Test (APT) complaint to SP800-90B section 4.4.2

2.8.3 Critical Function Tests

The module performs the following critical function tests in the UEFI OS Loader:

- RSA Signature Verification

The modules performs the following critical function tests on both the ISG OS and ISG:

- CTR DRBG Instantiate Critical Function Test
- CTR DRBG Reseed Critical Function Test
- CTR DRBG Generate Critical Function Test
- CTR DRBG Uninstantiate Critical Function Test

The ISG runs a health check on the CTR DRBGs every 2^24 requests, which is less than the CTR DRBG reseed interval of 2^48 per NIST SP800-90A.

Additionally, per the IG A.9 requirements**,** the ISG Cryptographic Library performs the following critical functions test for AES XTS to ensure that the two keys used in this operation are not identical (Key_1 ≠ Key_2):

- AES XTS Duplicate Key Test

2.9 Mitigation of Other Attacks

This section is not applicable. The module does not claim to mitigate any attacks beyond the Level 2 requirements for this validation.

3 Secure Operation

ISG can be configured into an explicit FIPS mode of operation as per the instructions provided in Section 3.2. However, ISG supports a non-compliant state, the initialization of which requires an explicit separate configuration. When ISG is operating in non-compliant state, the services have access to non-Approved and non-Allowed algorithms. The logical boundary of the module is defined such that all functionality available in non-compliant state is scoped out from the module boundary. Thus, when the module is operating in FIPS Approved mode of operation, it can access only FIPS Approved or Allowed algorithms as access to non-Approved and non-Allowed algorithms are explicitly inhibited by design of the module.

The module meets Level 2 requirements. The sections below describe how to place and keep the module in FIPS-Approved mode of operation. The tamper evident seals and shutter devices shall be installed for the module to operate in the Approved mode of operation.

3.1 Initial Setup for S410 Appliance

Before powering on the module, the Crypto Officer must ensure that the required temper-evident labels (included with the FIPS security kit) are correctly applied to the enclosure. The FIPS security kit for the module includes the following items shown in Figure 7.

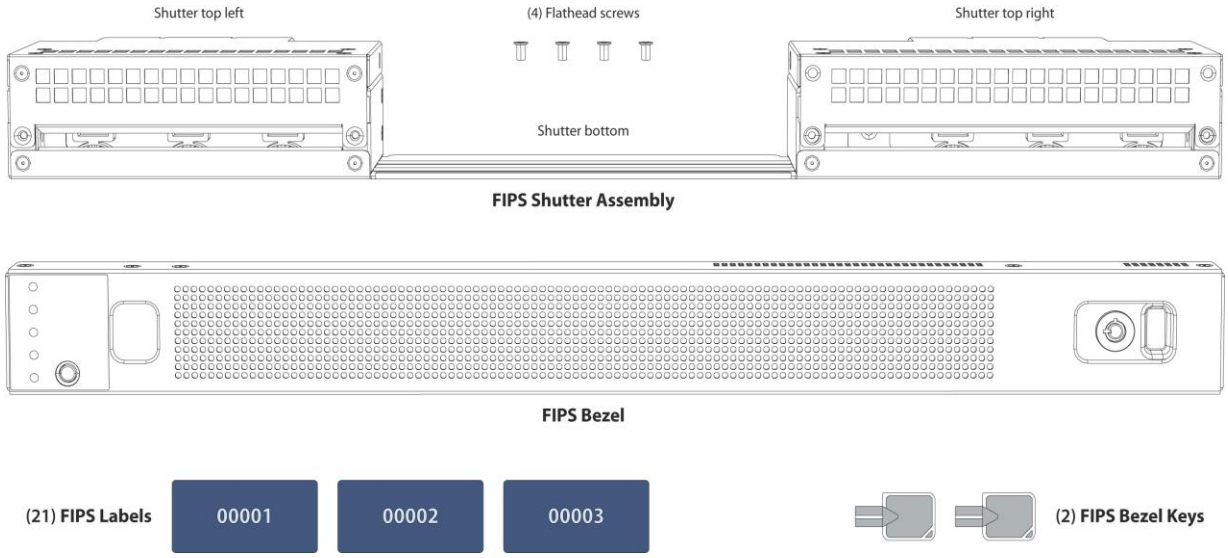

Figure 7 S410 FIPS Kit Contents

NOTE: Included with the S410 FIPS Kits are 21 blue labels. Only three labels are required for FIPS compliance. The additional labels are provided for reapplication purposes.

3.1.1 S410 Shutter, Bezel Cover, and Label Installation

The Crypto Officer is responsible for installing the baffle (security panel), installing the bezel cover, and applying the tamper evident labels at the client's deployment site to ensure full FIPS 140-2 compliance. Once the seals have been applied, the Crypto Officer must develop an inspection schedule to verify that the external enclosure of the module and the tamper seals have not been damaged or tampered with in any way. The Crypto Officer is

responsible for securing and having control at all times of any unused labels. The Crypto Officer is responsible for the direct control and observation of any changes to the module such as reconfigurations where the tamper-evident labels or security appliances are removed or installed to ensure the security of the module is maintained during such changes and the module is returned to a FIPS Approved state.

The steps for FIPS installation are documented in the following sections:

- "SSP-S410 FIPS Shutter Installation" in section 3.1.1.1
- "SSP-S410 FIPS Bezel Cover Installation" in section 3.1.1.2
- "SSP-S410 FIPS Label Application" in section 3.1.1.3

3.1.1.1 S410 FIPS Shutter Installation

The FIPS shutter prevents unauthorized access to the appliance's console, management, and Ethernet ports, and the PCIe option cards. The shutter is comprised of three pieces (upper left, upper right, and lower) and must be disassembled before it attached to the chassis. Instructions for installing the FIPS modules are shown below in Figure 8 and Figure 9 and Figure 10.

To install the FIPS shutter:

1. Disassemble the FIPS shutter:

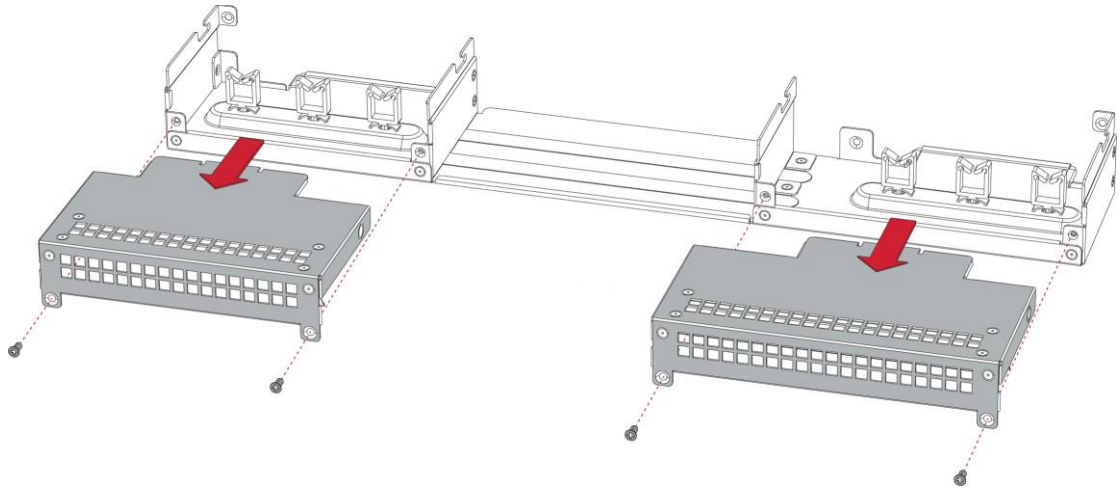

Figure 8 Disassemble the S410 FIPS Shutter

- Remove the two screws securing the left upper shutter and gently pull the upper shutter rearward.
- Set the left shutter and two screws aside in a safe place.
- Repeat these steps to remove the right upper shutter.

2. Attach the lower shutter to the appliance:

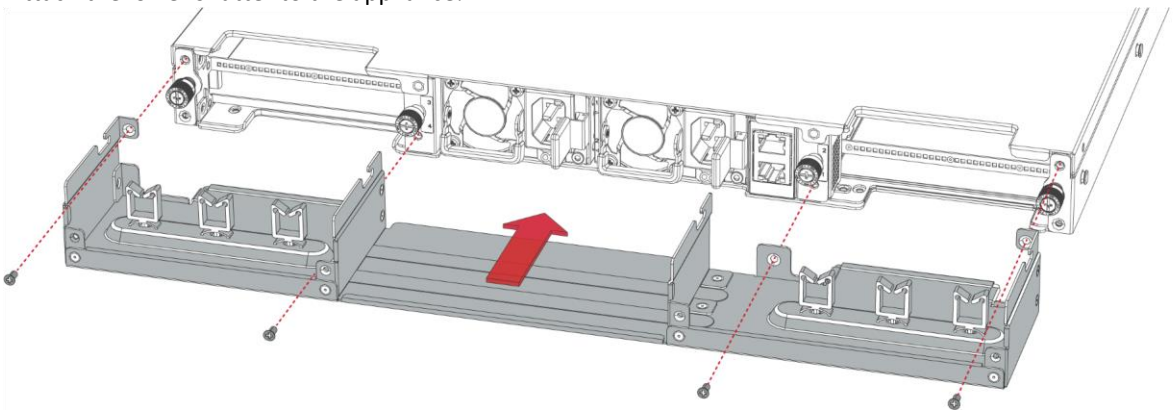

Figure 9 Attach the S410 Lower Shutter

- Align the lower shutter's mounting points with the screw holes in the chassis.
- Secure the lower shutter with the four screws, two on each side, included with the FIPS kit.

3. Mount the appliance in an equipment rack. Refer to the appliance's user guide for installation and safety instructions.

4. Reinstall the appliance network and other interconnect cables to their respective locations.

NOTE: All network and interconnect cables must installed at this time to prevent reopening of the shutters and subsequent reapplication of the security labels.

5. Route the network cables through the cable management anchors to prevent cables from obstructing airflow.

6. Attach the left and right upper shutters to the lower shutter:

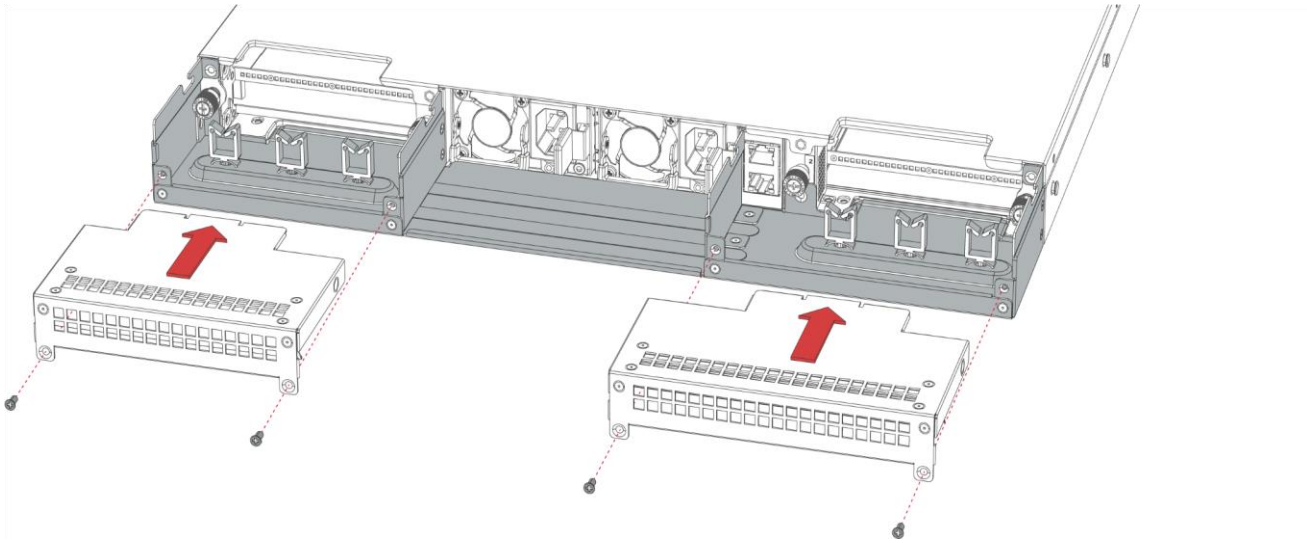

Figure 10 Attach S410 left and right Upper Shutters

- Align the left upper shutter's mounting points with the screw holes in the lower shutter.
- Secure the left upper shutter with the two screws previously removed.
- Repeat these steps to attach the right upper shutter.

3.1.1.2 S410 FIPS Bezel Cover Installation

The FIPS bezel cover prevents unauthorized access to the appliance's drives and front-panel switches. The bezel cover is locked with the FIPS bezel key. Bezel Cover Installation is shown below in Figure 11 and Figure 12.

To install the FIPS bezel cover:

1. Verify the following:
   - The rear shutter is installed (see "S410 FIPS Shutter Installation" in section 3.1.1.1).
   - The appliance is mounted in the equipment. Refer to the appliance's user guide for installation and safety instructions.
2. If necessary, slide the appliance out of the rack to better access the front of the chassis.
3. Align the left side of the bezel cover with the left attachment bracket, inserting the bezel cover's two mounting posts into the holes in the attachment bracket.
4. Align the right side of the bezel cover with the right attachment bracket, inserting the bezel cover's two mounting posts into the holes in the attachment bracket.

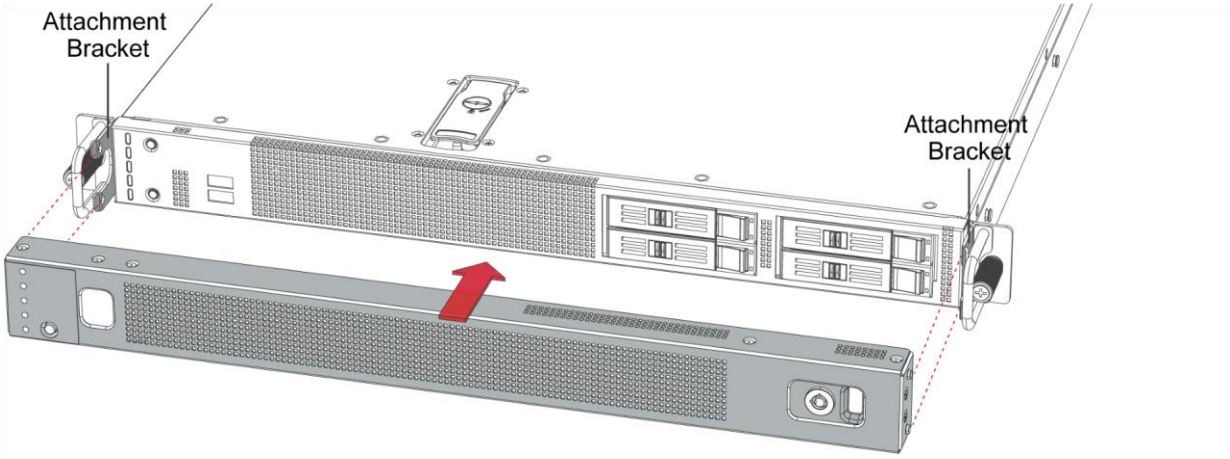

Figure 11 Attach the S410 Bezel Cover

5. Push gently on the bezel cover until it snaps into place, with the four mounting posts (two per edge)
6. Insert the bezel key in the key lock and turn it clockwise until it locks in place.

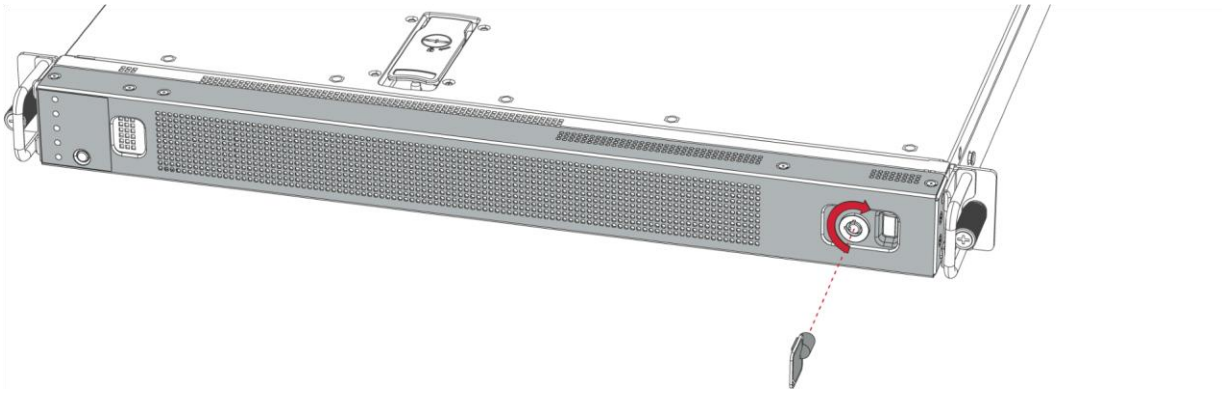

Figure 12 Lock the S410 cover

7. Remove the bezel key and store it in a safe place.

3.1.1.3 S410 FIPS Label Application

The FIPS compliant labels are applied over key areas of the chassis to provide tamper-evident security. If the labels are removed after being affixed to a surface, the image self-destructs and leaves a pattern of VOID markings on the label. Figure 13 illustrates the tamper-evident features of the label.

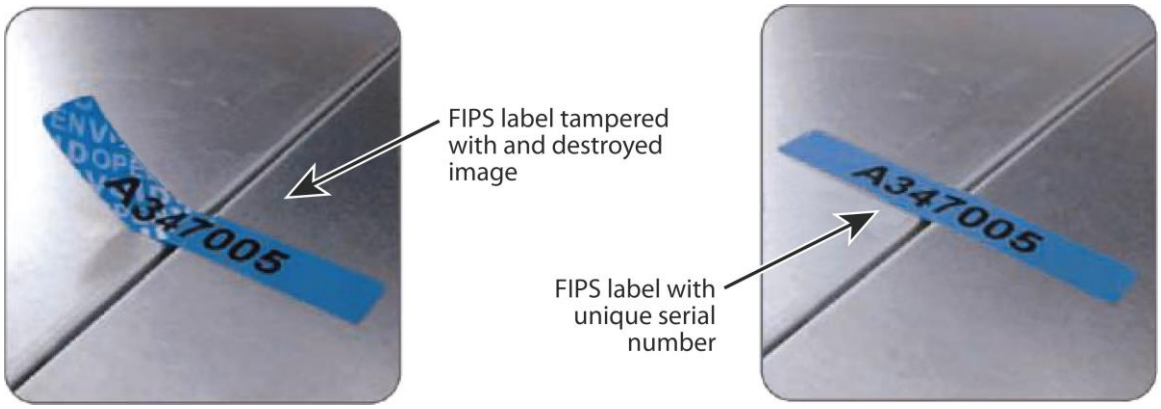

Figure 13 FIPS Label Showing Tamper Evidence

WARNING! Crypto Officers must adhere to the following guidelines when applying the tamper-evident labels:

- The minimum temperature of the environment is 35 degrees Fahrenheit. After application, the labels' acceptable temperature in the operational environment is –5 degrees to 158 degrees Fahrenheit.
- Do not touch the adhesive side of the label. This disrupts the integrity of the adhesive. If a label is removed from a surface, the image is destroyed and the label shows tamper-evident text as evidence. If you accidentally touch the adhesive side, discard that label and apply another one.
- Use alcohol swabs to clean the label location surface with isopropyl alcohol (99%); this ensures complete adhesion. Verify that all the surfaces are dry before applying the labels.

NOTE: Label application tips:

- Apply skin moisturizer on your fingers before handling.
- Use a rubber fingertip to partially remove the label from its backing.
- After applying the labels, allow at least 24 hours for the label adhesive to cure.

To apply the FIPS labels:

1. Verify the following:
   - The rear shutter is installed (see "S410 FIPS Shutter Installation" in section 3.1.1.1).
   - The appliance is mounted in the equipment (see the appliance's user guide for installation and safety instructions).
   - The bezel cover is installed (see "S410 FIPS Bezel Cover Installation" in section 3.1.1.2).
2. Apply one label to the FIPS bezel over the key lock.
3. Apply two labels (one each) to the left and right upper shutters. Place the labels so they extend from the shutters to the rear edge of the appliance cover.

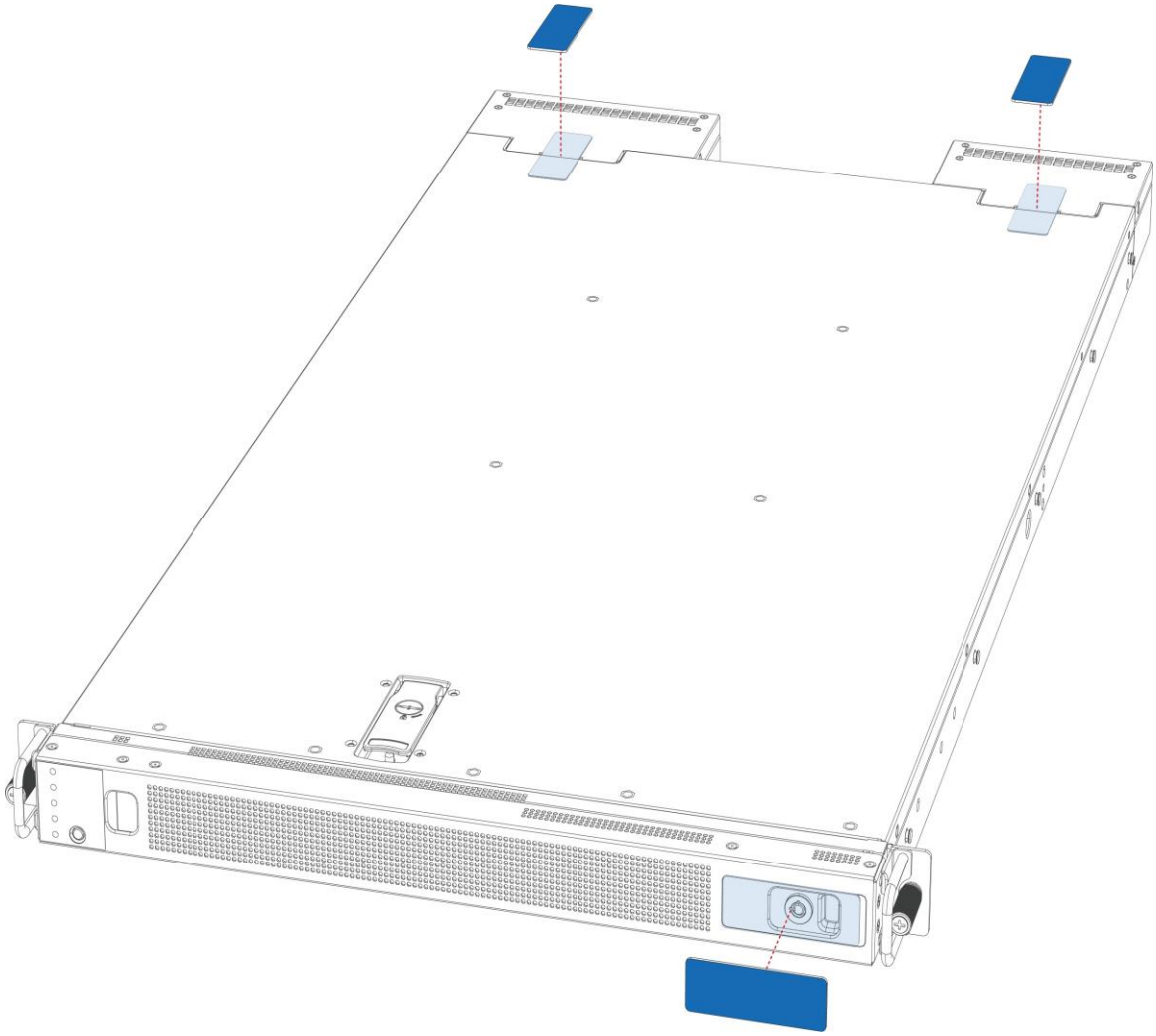

Figure 14 Apply S410 Labels

1. **WARNING!** The rear FIPS labels are destroyed each time the appliance cover is removed. Make sure to re-secure the appliance after servicing. Application of labels is shown in Figure 14Set the appliance on a flat, slip-proof space and make sure you have access to all sides of the appliance.
2. Apply two (2) short labels (short labels 1 and 2) over the exposed shutter screw heads. These labels extend slightly over the left and right edges of the shutter when properly applied.
3. Power-on the appliance by plugging in the power cords.

3.2 Initial Setup for S210 Appliance

Before powering on the module, the Crypto Officer must ensure that the required temper-evident labels (included with the FIPS security kit) are correctly applied to the enclosure. The FIPS security kit for the module includes the following items shown in Figure 7.

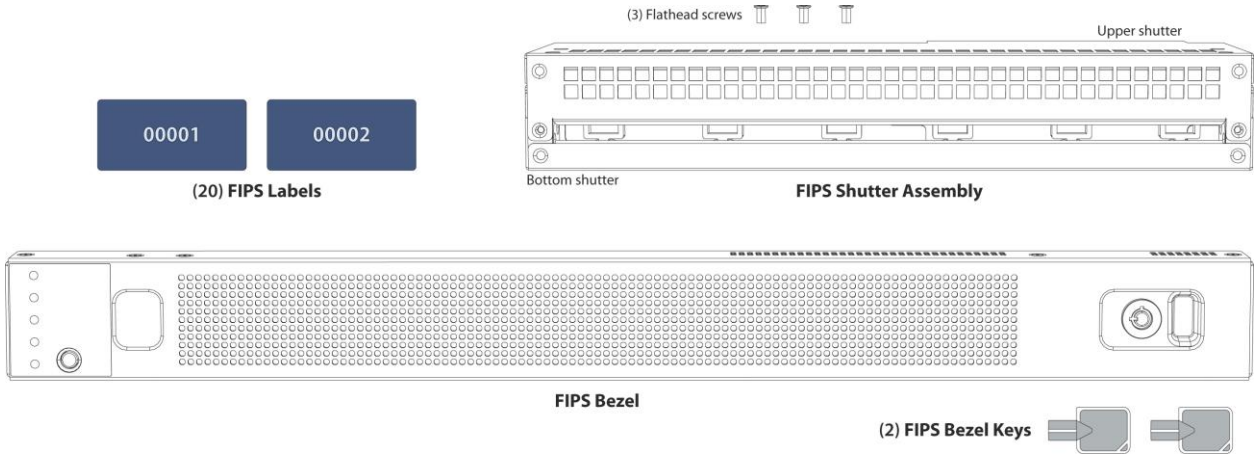

Figure 15 S210 FIPS Kit Contents

NOTE: Included with the S210 FIPS Kits are 21 blue labels. Only two labels are required for FIPS compliance. The additional labels are provided for reapplication purposes.

3.2.1 S210 Shutter, Bezel Cover, and Label Installation

The Crypto Officer is responsible for installing the baffle (security panel), installing the bezel cover, and applying the tamper evident labels at the client's deployment site to ensure full FIPS 140-2 compliance. Once the seals have been applied, the Crypto Officer must develop an inspection schedule to verify that the external enclosure of the module and the tamper seals have not been damaged or tampered with in any way. The Crypto Officer is responsible for securing and having control at all times of any unused labels. The Crypto Officer is responsible for the direct control and observation of any changes to the module such as reconfigurations where the tamper-evident labels or security appliances are removed or installed to ensure the security of the module is maintained during such changes and the module is returned to a FIPS Approved state.

The steps for FIPS installation are documented in the following sections:

- "SSP-S210 FIPS Shutter Installation" in section 3.2.1.1
- "SSP-S210 FIPS Bezel Cover Installation" in section 3.2.1.2

- "SSP-S210 FIPS Label Application" in section 3.2.1.3

3.2.1.1 S210 FIPS Shutter Installation

The FIPS shutter prevents unauthorized access to the appliance's console, management, and Ethernet ports, and the PCIe option cards. The shutter is comprised of two pieces (upper and lower) and must be disassembled before it attached to the chassis. Instructions for installing the FIPS modules are shown below in Figure 16 and Figure 17 and Figure 18.

To install the FIPS shutter:

1. Disassemble the FIPS shutter:

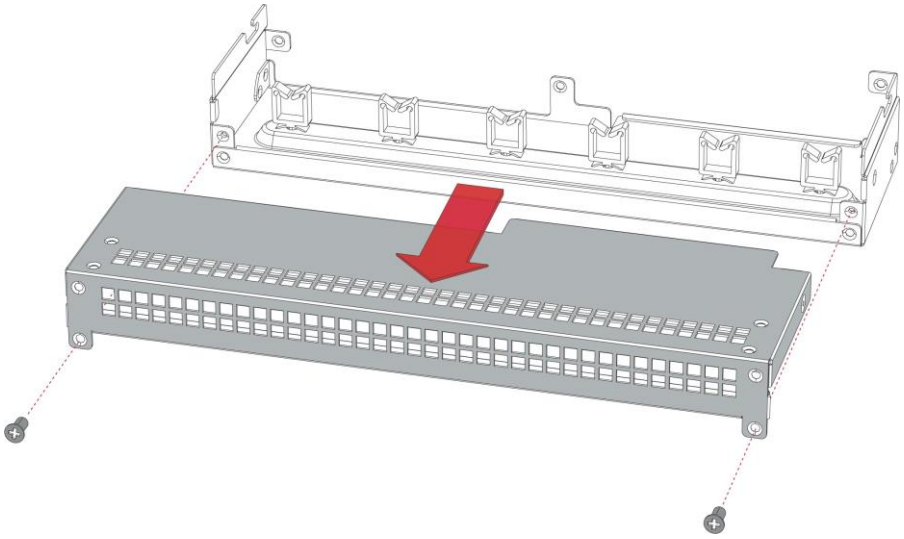

Figure 16 Disassemble the S210 FIPS Shutter

- Remove the two screws securing the shutter and gently pull the upper shutter rearward.
- Set the shutter and screws aside in a safe place.

2. Attach the lower shutter to the appliance:

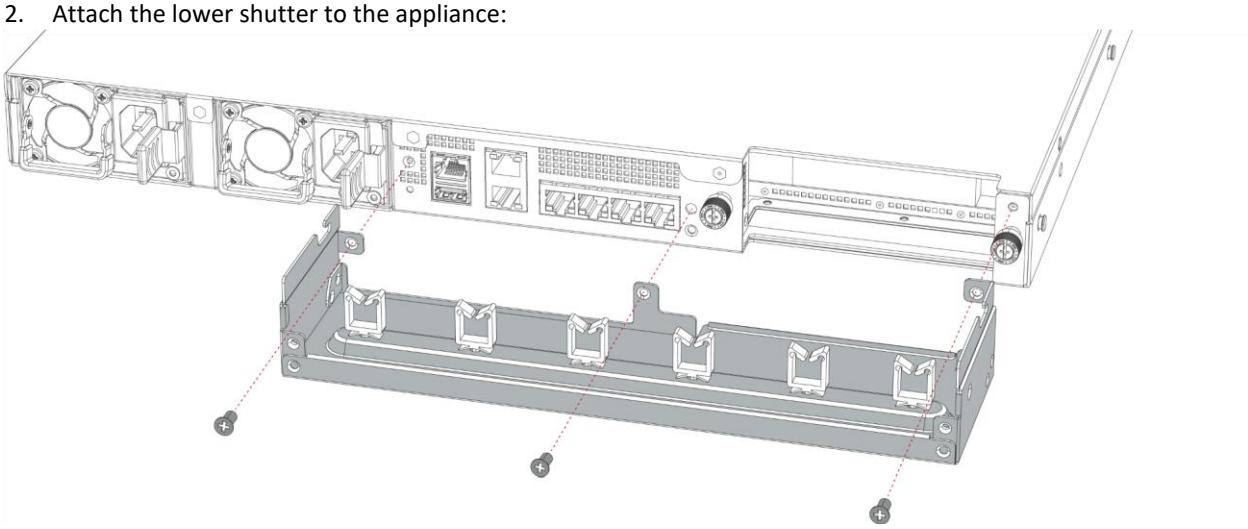

Figure 17 Attach the S210 Lower Shutter

- Align the lower shutter's mounting points with the screw holes in the chassis.
- Secure the lower shutter with the four screws, two on each side, included with the FIPS kit.

3. Mount the appliance in an equipment rack. Refer to the appliance's user guide for installation and safety instructions.

4. Reinstall the appliance network and other interconnect cables to their respective locations.

NOTE: All network and interconnect cables must installed at this time to prevent reopening of the shutters and subsequent reapplication of the security labels.

5. Route the network cables through the cable management anchors to prevent cables from obstructing airflow.

6. Attach the upper shutter to the lower shutter:

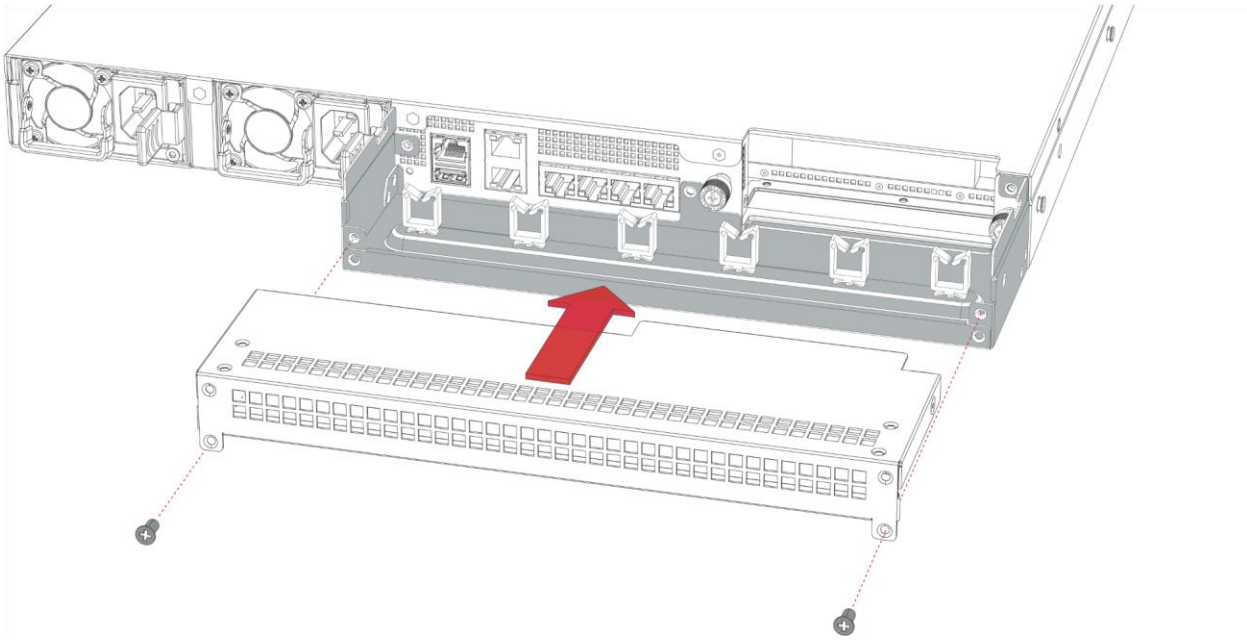

Figure 18 Attach S210 Upper Shutter

- Align the upper shutter's mounting points with the screw holes in the lower shutter.
- Secure the upper shutter with the two screws previously removed.

3.2.1.2 S210 FIPS Bezel Cover Installation

The FIPS bezel cover prevents unauthorized access to the appliance's drives and front-panel switches. The bezel cover is locked with the FIPS bezel key. Bezel Cover Installation is shown below in Figure 11 and Figure 12.

To install the FIPS bezel cover:

1. Verify the following:
   - The rear shutter is installed (see "S210 FIPS Shutter Installation" in section 3.2.1.1).
   - The appliance is mounted in the equipment. Refer to the appliance's user guide for installation and safety instructions.
2. If necessary, slide the appliance out of the rack to better access the front of the chassis.
3. Align the left side of the bezel cover with the left attachment bracket, inserting the bezel cover's two mounting posts into the holes in the attachment bracket.
4. Align the right side of the bezel cover with the right attachment bracket, inserting the bezel cover's two mounting posts into the holes in the attachment bracket.

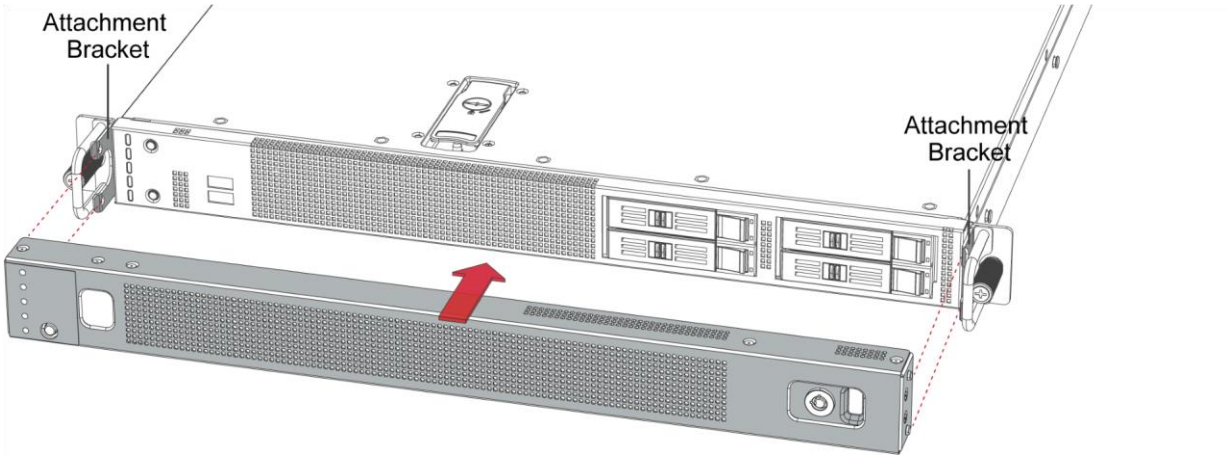

Figure 19 Attach the S210 Bezel Cover

5. Push gently on the bezel cover until it snaps into place, with the four mounting posts (two per edge)
6. Insert the bezel key in the key lock and turn it clockwise until it locks in place.

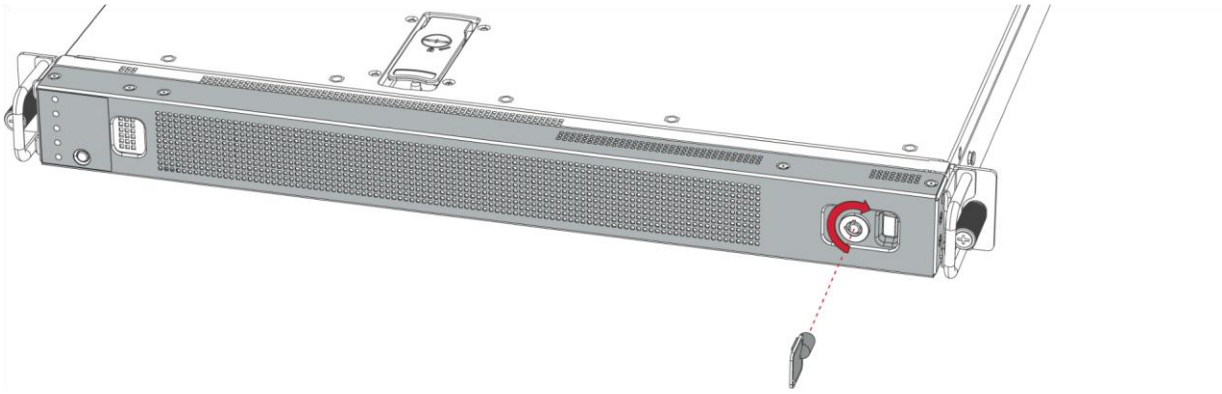

Figure 20 Lock the S210 cover

7. Remove the bezel key and store it in a safe place.

3.2.1.3 S210 FIPS Label Application

The FIPS compliant labels are applied over key areas of the chassis to provide tamper-evident security. If the labels are removed after being affixed to a surface, the image self-destructs and leaves a pattern of VOID markings on the label. Figure 21 illustrates the tamper-evident features of the label.

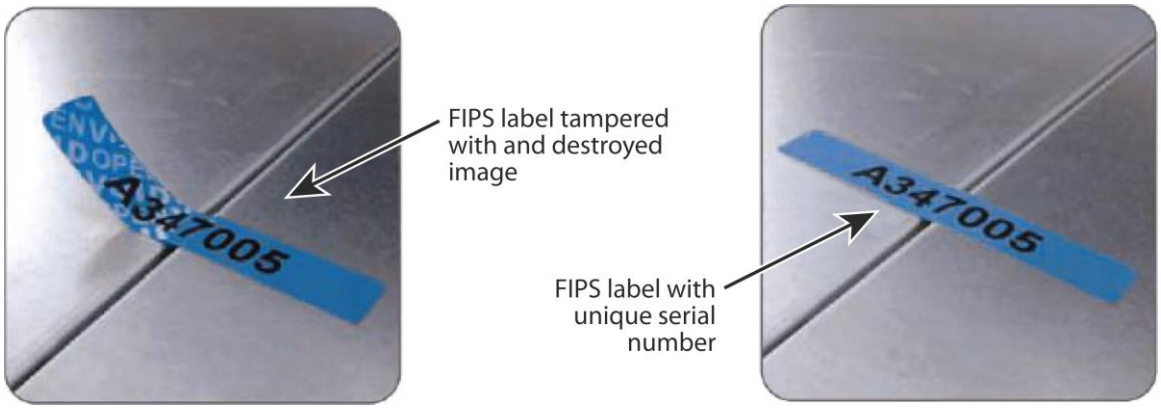

Figure 21 FIPS Label Showing Tamper Evidence

WARNING! Crypto Officers must adhere to the following guidelines when applying the tamper-evident labels:

- The minimum temperature of the environment is 35 degrees Fahrenheit. After application, the labels' acceptable temperature in the operational environment is –5 degrees to 158 degrees Fahrenheit.
- Do not touch the adhesive side of the label. This disrupts the integrity of the adhesive. If a label is removed from a surface, the image is destroyed and the label shows tamper-evident text as evidence. If you accidentally touch the adhesive side, discard that label and apply another one.
- Use alcohol swabs to clean the label location surface with isopropyl alcohol (99%); this ensures complete adhesion. Verify that all the surfaces are dry before applying the labels.

NOTE: Label application tips:

- Apply skin moisturizer on your fingers before handling.
- Use a rubber fingertip to partially remove the label from its backing.
- After applying the labels, allow at least 24 hours for the label adhesive to cure.

To apply the FIPS labels:

1. Verify the following:
   - The rear shutter is installed (see "S210 FIPS Shutter Installation" in section 3.2.1.1).
   - The appliance is mounted in the equipment (see the appliance's user guide for installation and safety instructions).
   - The bezel cover is installed (see "S210 FIPS Bezel Cover Installation" in section 3.2.1.2).
2. Apply one label to the FIPS bezel over the key lock.
3. Apply one label to the upper shutter. Place the label so it extends from the shutter to the rear edge of the appliance cover.

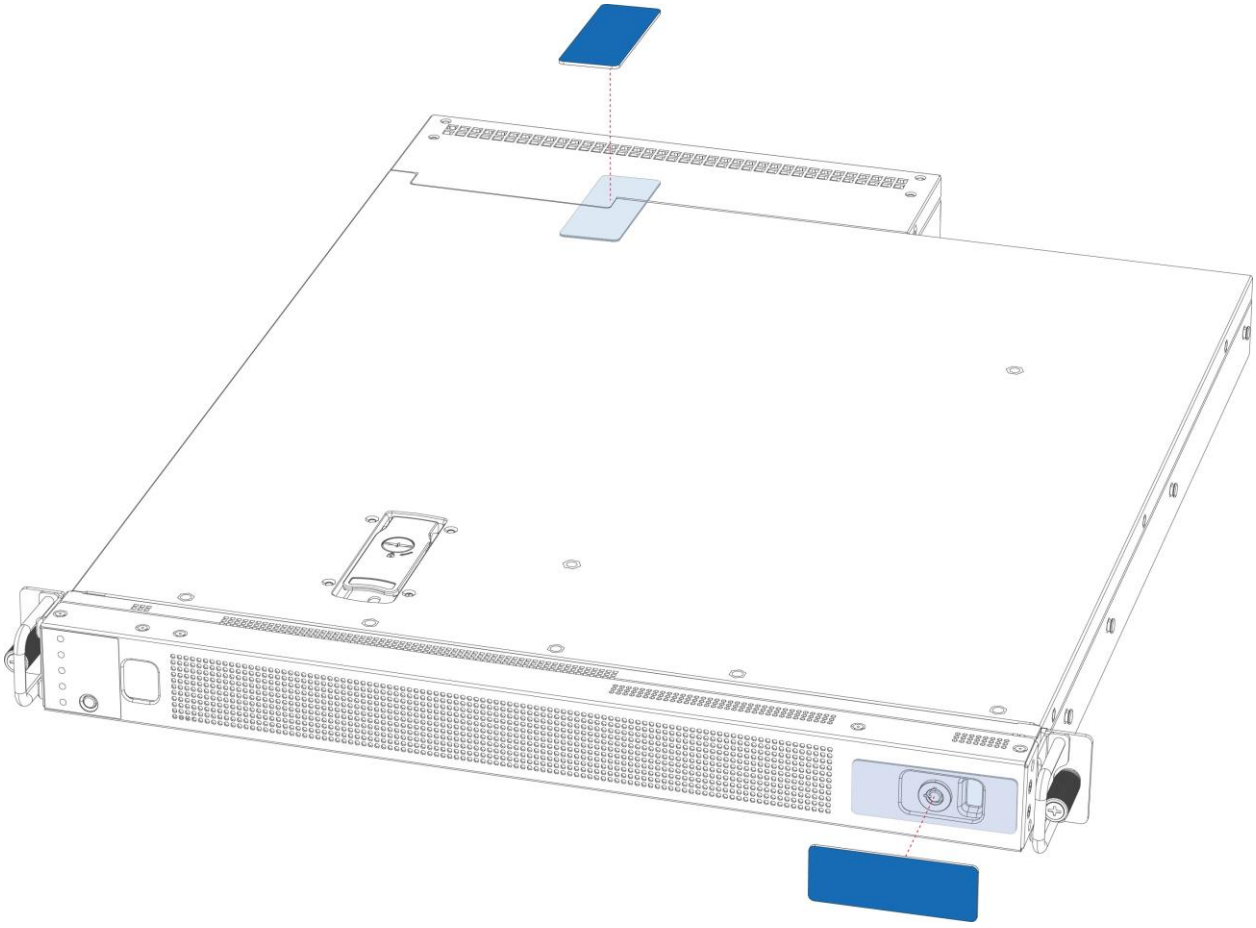

Figure 22 Apply S210 Labels

WARNING! The rear FIPS labels are destroyed each time the appliance cover is removed. Make sure to re-secure the appliance after servicing. Application of the labels is shown in Figure 22.

4. Set the appliance on a flat, slip-proof space and make sure you have access to all sides of the appliance.
5. Apply one (1) short label over the exposed shutter screw head. This label extend slightly over the left and right edges of the shutter when properly applied.
6. Power-on the appliance by plugging in the power cords.

3.3 Secure Management

3.3.1 Initialization

The module is delivered in an uninitialized factory state, and requires minimal first-time configuration to operate in FIPS-Approved mode and be accessed remotely. Physical access to the module shall be limited to the Crypto-Officer (CO), and the CO shall be responsible for putting the module into the Approved mode. Note, these same steps in this section shall be followed after the zeroization command is entered.

The process of establishing the initial configuration via a secure serial port is described below.

1. Connect a serial cable to a PC and to the module's serial port. Open a terminal emulator (such as HyperTerminal) on the PC, and connect to the serial port to which you attached the cable. Create and name a new connection (either a COM or TCP/IP), using the port parameters provided in Table 16.

Table 16 RS-232 Parameters

RS-232C Parameter	Parameter Setting
Baud rate	9600 bps
Data bits	8
Parity	None
Stop bits	1
Flow control	None

2. Power up the module and wait for the system to finish booting.
3. Press **Enter** three times.

```
Welcome to the Symantec S410 Series Appliance Serial Console
Version: ISG 2.4.2.1, Release id: 272516 64-bit

------------------------- MENU ------------------------------
1) Command Line Interface
2) Setup Console
-------------------------------------------------------------
Enter option:
```

4. Enter **1** to access the Command Line Interface.
5. Type **enable** and press **Enter**.
6. Enter the following command: **fips-mode enable**.

   When prompted for confirmation, select **Y** to confirm

   - **NOTE 1**: The fips-mode enable command causes the device to power cycle, zeroing the appliance and returning the configuration values set in steps 1 and 2 to their factory state.

7. After the system has finished rebooting, press **Enter** three times.
8. Enter **2** to access the Setup Console.
9. Enter the properties for the following:

a. Interface number
b. Enter 'No' for DHCP
c. IP address
d. IP subnet mask
e. IP gateway
f. DNS server parameters

10. The module will prompt for the console account credentials:

```
DIRECTIONS:
The console username, password and enable password are special
administrative credentials which can be used to log into the command
line interface.

Enter console password:
Verify console password:

Enter enable password:
Verify enable password:
```

11. The module will report that is in FIPS mode and the serial console must be configured:

```
Enter serial setup password:
Verify serial setup password:
```

Upon completion of these initialization steps, the module is considered to be operating in its Approved mode of operation. There are no additional non-Approved services while operating in the Approved mode.

3.3.2 Management

The Crypto-Officer is able to monitor and configure the module via the CLI (serial port or SSH).

The Crypto-Officer should monitor the module's status regularly. If any irregular activity is noticed or the module is consistently reporting errors, customers should consult Symantec's Product Documentation portal and the administrative guidance documents to resolve the issues. If the problems cannot be resolved through these resources, Symantec customer support should be contacted.

If the CO detects signs of physical tampering, then the module is no longer operating in the Approved mode and must be taken out of service.

The CO password and "enabled" mode password must be at least 8 characters in length.

3.3.3 Zeroization

The CO can return the module to its uninitialized factory state by entering the "enabled" mode on the CLI, followed by the "`fips-mode disable`" command. This command will automatically reboot the module and zeroize all keys. Zeroization includes all temporary/ephemeral session keys, and also the persistently stored RSA private key, Crypto-Officer password, User password, and "Enabled" mode password. The Crypto-Officer must wait until the module has successfully rebooted in order to verify that zeroization has completed.

3.4 User Guidance

The User is only able to access the module remotely via SSH (CLI). The User must change his or her password at the initial login. The User must be diligent to pick strong passwords (alphanumeric with minimum 8 characters) that will not be easily guessed and must not reveal their password to anyone. Additionally, the User should be careful to protect any secret/private keys in their possession, such as TLS or SSH session keys. The User should report to the Crypto-Officer if any irregular activity is noticed.

4 Acronyms

This section describes the acronyms used throughout this document. See Table 17 below.

Table 17 Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CO	Crypto-Officer
CRNGT	Continuous Random Number Generator Test
CCCS	Canadian Centre for Cyber Security
CSP	Critical Security Parameter
DNS	Domain Name System
DRBG	Deterministic Random Bit Generator
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
HMAC	Hash-Based Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Secure Hypertext Transfer Protocol
KAT	Known Answer Test
LCD	Liquid Crystal Display
LED	Light Emitting Diode
NIST	National Institute of Standards and Technology
NP	Non-Physical
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm
SSH	Secure Shell
TLS	Transport Layer Security
USB	Universal Serial Bus