

**Huawei S7700 Series Switches**

# **Non-Proprietary FIPS 140-2 Security Policy**

**Issue**        1.1  
**Date**        2017-07-26

**Copyright © Huawei Technologies Co., Ltd. 2017.**

This document may be reproduced only in its original entirety [without revision].

## **Trademarks and Permissions**



and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

## **Notice**

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

## **Huawei Technologies Co., Ltd.**

Address: Huawei Industrial Base  
Bantian, Longgang  
Shenzhen 518129  
People's Republic of China

Website: <http://e.huawei.com>

# Contents

---

<b>1</b>	<b>References and Definitions .....</b>	<b>1</b>
<b>2</b>	<b>Introduction .....</b>	<b>3</b>
2.1	Security Levels.....	6
2.2	Modes of Operation .....	6
<b>3</b>	<b>Ports and Interfaces .....</b>	<b>7</b>
<b>4</b>	<b>Cryptographic Functionality.....</b>	<b>15</b>
4.1	Critical Security Parameters and Public Keys.....	19
<b>5</b>	<b>Roles, Authentication and Services.....</b>	<b>20</b>
5.1	Assumption of Roles.....	20
5.2	Authentication Methods.....	20
5.3	Services .....	21
<b>6</b>	<b>Self-tests.....</b>	<b>24</b>
<b>7</b>	<b>Physical Security Policy.....</b>	<b>25</b>
7.1	Tamper Seal Placement.....	25
7.1.1	S7703.....	25
7.1.2	S7706.....	26
7.1.3	S7712.....	28
<b>8</b>	<b>Operational Environment .....</b>	<b>32</b>
<b>9</b>	<b>Mitigation of Other Attacks Policy .....</b>	<b>33</b>
<b>10</b>	<b>Security Rules and Guidance .....</b>	<b>34</b>

# 1 References and Definitions

**Table 1-1: References**

Ref	Full Specification Name
ESP	Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, Internet Engineering Task Force, December 2005.
ESP-B	Law, L. and J. Solinas, "Suite B Cryptography Suites for IPsec", RFC 6379, Internet Engineering Task Force, October 2011.
LDAP	Semersheim, J., Ed., "Lightweight Directory Access Protocol (LDAP): The Protocol", RFC 4511, Internet Engineering Task Force, June 2006.
RADIUS	Rigney, C., Rubens, A., Simpson, W. and S. Willens, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, Internet Engineering Task Force, June 2000.
SSH	Ylonen, T. and C. Lonvick, "The Secure Shell (SSH) Connection Protocol", RFC 4254, Internet Engineering Task Force, January 2006.
SSH-B	K. Igoe, "Suite B Cryptography in Suites for Secure Shell (SSH)", Internet Engineering Task Force, May 2011.
TLS	Dierks, T., and E. Rescoria, "The Transport Layer Security (TLS) Protocol Version 1.2". RFC 5246, Internet Engineering Task Force, August 2008.
TLS-B	Salter, M and R. Housely, "Suite B Profile for Transport Layer Security (TLS)", Internet Engineering Task Force, January 2012.

**Table 1-2: Acronyms and Definitions (for terms not defined in FIPS 140-2 and associated documents)**

Term	Definition
AAA	Authentication, Authorization and Accounting - access control, policy enforcement and auditing framework for computing systems, e.g. LDAP
BCM	Broadcom
ESP	Encapsulated Security Payload (a subset of IPsec, Internet Protocol Security)
eSAP	Enterprise Service Application Platform
GUI	Graphical User Interface
HFCL	Huawei FIPS Cryptographic Library
IETF	Internet Engineering Task Force, a standards body
IPC	Inter-process Communication
IPOS	IP Operating System
L2MC	Layer 2 MultiCast
LDAP	Lightweight Directory Access Protocol
LPU	Line Processing Unit
MPU	Main Processing Unit

Term	Definition
MVL	Marvel
RFC	Request For Comment; the prefix used by IETF for internet specifications.
SFU	Switched Fabric Unit
SSH	Secure Shell
VPN	Virtual Private Network
VRP	Versatile Routing Platform
TLS	Transport Layer Security
TSM	Terminal Security Management
UDP	User Datagram Protocol

## 2 Introduction

The Huawei SWITCH are multi-chip standalone cryptographic modules enclosed in hard, commercial grade metal cases. The cryptographic boundary for these modules is the enclosure. The primary purpose of these modules is to provide secure communication for data transmitted between different networks. The modules provide network interfaces for data input and output. The appliance encryption technology uses FIPS approved algorithms. FIPS approved algorithms are approved by the U.S. government for protecting Unclassified data.

The module is designated as a limited operational environment under the FIPS 140-2 definitions. The module includes a firmware load service to support necessary updates. New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into this module is out of the scope of this validation and require a separate FIPS 140-2 validation.

**Table 2-1: Cryptographic Module Configurations**

Module (Base Model)*	HW P/Ns and Versions	FW Version
S7703	Base Model P/N: 02113959 Version: P.3 Main Processing Unit (MPU) P/N: 03030MPV (Qty. 2) Line Processing Unit (LPU) P/N: 03030MQP Tamper Seals P/N: 4057-113016	V200R010C00SPC900B900
S7706	Base Model P/N: 02113960 Version: N.2 MPU P/N: 03030MQS (Qty. 2) CSS P/N: 03030QHL(Qty. 2) LPU P/N: 03030MQP Tamper Seals P/N: 4057-113016	V200R010C00SPC900B900
S7712	Base Model P/N: 02113961 Version: P.2 MPU P/N: 03031FSL (Qty. 2) CSS P/N: 03030XYD (Qty. 2) LPU P/N: 03030MQP Tamper Seals P/N: 4057-113016	V200R010C00SPC900B900

\* Note that the FIPS validated configuration is the base model with the following interface cards installed:

- Main Processing Unit (MPU) interface cards
- Content Services Switch (CSS) interface cards (applicable for S7706 and S7712 models only)
- Line Processing Unit (LPU) interface card

Unpopulated card slots are covered by faceplates. Each interface card and faceplate is protected with tamper-evident seals (refer to Section 7.1).

Figure 2-1: – Figure 2-6: show the cryptographic boundary of the module.



**Figure 2-1: S7703 (Top, Right, Front)**



**Figure 2-2: S7703 (Bottom, Left, Back)**



**Figure 2-3: S7706 (Top, Left, Front)**



**Figure 2-4: S7706 (Bottom, Right, Back)**



Figure 2-5: S7712 (Top, Left, Front)



Figure 2-6: S7712 (Bottom, Right, Back)

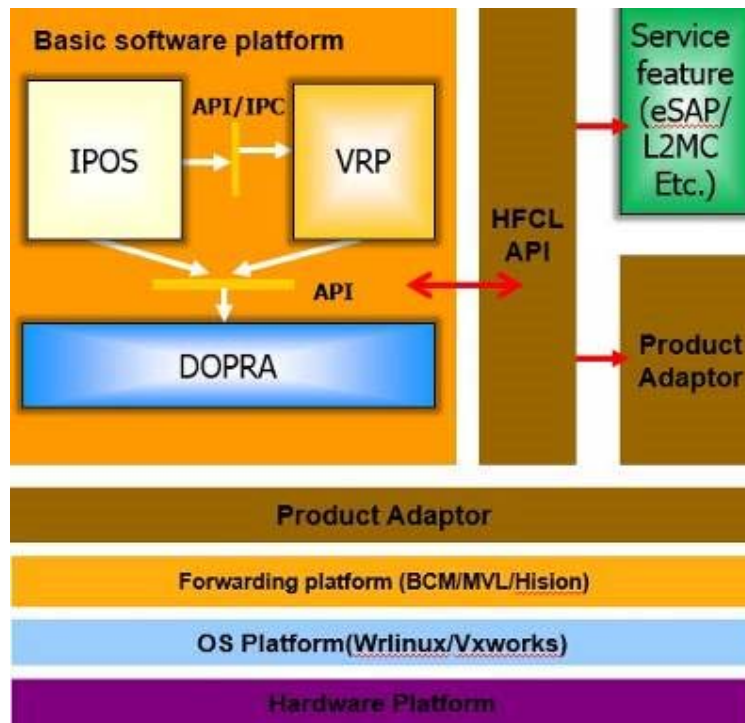


Figure 2-7: Firmware Block Diagram



## 2.1 Security Levels

The FIPS 140-2 security levels for the module are as follows:

**Table 2-2: Security Level of Security Requirements**

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

## 2.2 Modes of Operation

The module supports both an Approved and non-Approved mode of operation. By default, the module comes configured in the non-Approved mode.

See Section 10, *Security Rules and Guidance* for instructions on how to configure the module to function in the Approved mode operation.

### 3 Ports and Interfaces

The S7700 Series Switches provide a number of physical and logical interfaces, and the physical interfaces provided by the module are mapped to the four FIPS 140-2 defined logical interfaces: data input, data output, control input, and status output. The logical interfaces and their mapping are described in the tables below.

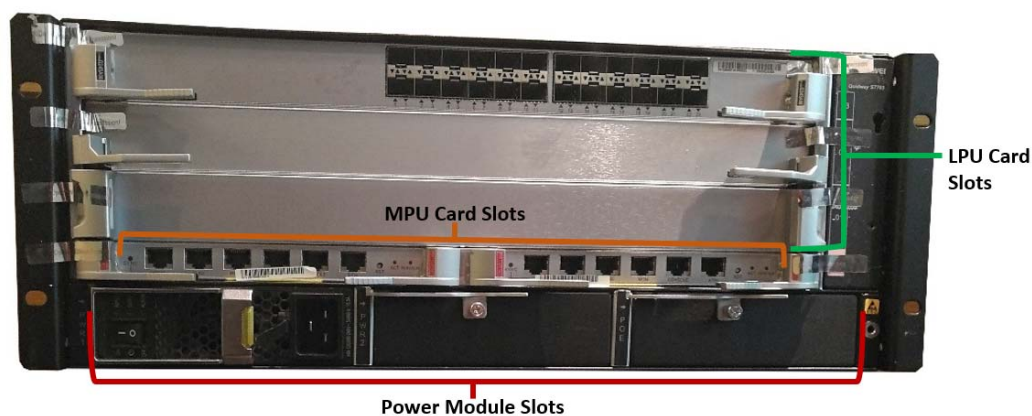


Figure 3-1: S7703 Ports – Front Panel

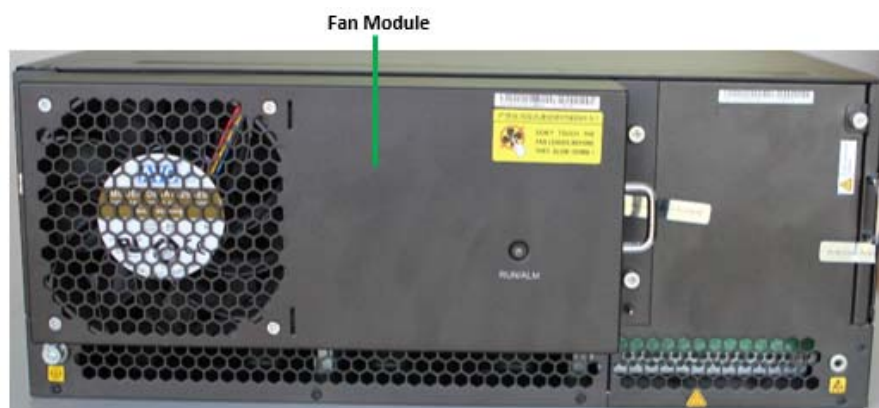


Figure 3-2: S7703 Ports – Back Panel

Table 3-1: S7703 Ports and Interfaces

Qty.	Port	Description	Logical Interface Type
2	MPU Card Slots	Main Processing Unit connection	Control in, data in, data out, status out. See Table 3-3.
3	LPU Card Slots <sup>1</sup>	Network traffic	Control in, data in, data out, status out. See Table 3-2.
3	Power Module Slots	Power	Power
1	Fan Module	Fan slot	N/A

<sup>1</sup> In the FIPS configuration, 1 LPU card is installed and the rest of the slots are covered with a faceplate.

The FIPS validated configuration for each model includes the following Line Processing Unit (LPU) with the following ports and interfaces:



Figure 3-3: S7703 / S7706 / S7712 LPU Card Ports

Table 3-2: S7703 / S7706 / S7712 LPU Card Ports and Interfaces Mapping

Port	Description	Logical Interface Type
1. GE/XGE/40GE/100GE ports (Qty. 24)	Copper or fiber Service ports	Control in, data in, data out, status out
LEDs	LINK/ACT, RUN/ALM LEDs	Status out

The FIPS validated configuration for the S7703 model includes two Main Processing Units (MPUs) with the following ports and interfaces:

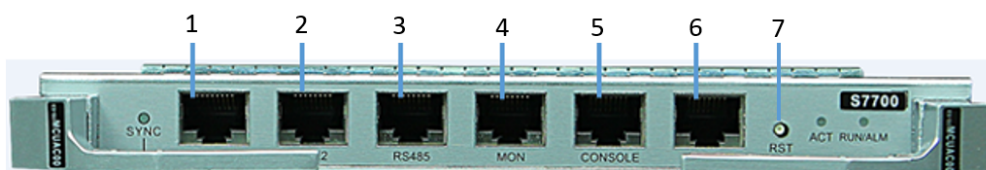


Figure 3-4: S7703 MPU Card

Table 3-3: S7703 MPU Card Ports and Interfaces Mapping

Port	Description	Logical Interface Type
1. CLK1	Clock in/out	Data in, data out
2. CLK2	Clock in/out	Data in, data out
3. RS485	Reserved	N/A
4. MON	Reserved	N/A
5. Console	Serial console via RJ45 & miniUSB	Control in, data in, data out, status out
6. ETH management port	Management Ethernet interface	Control in, data in, data out, status out
7. RST Button	Reset the card	Control in
LEDs	ACT, Run/ALM, SYNC LEDs	Status out

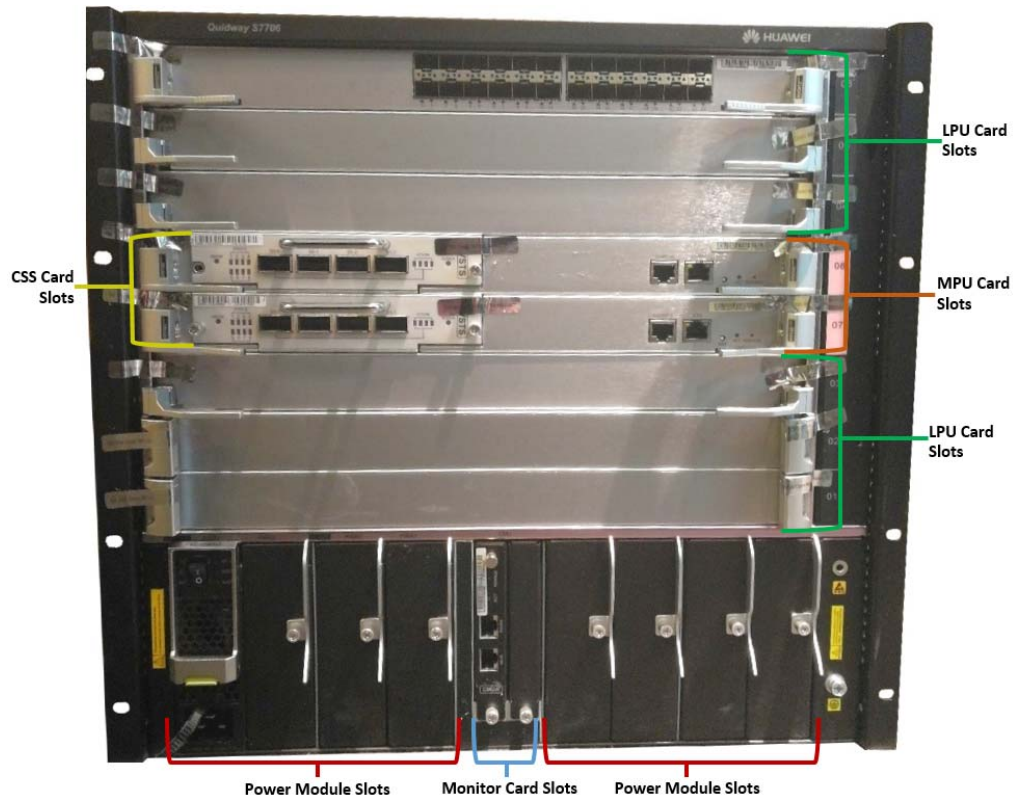


Figure 3-5: S7706 Ports – Front Panel

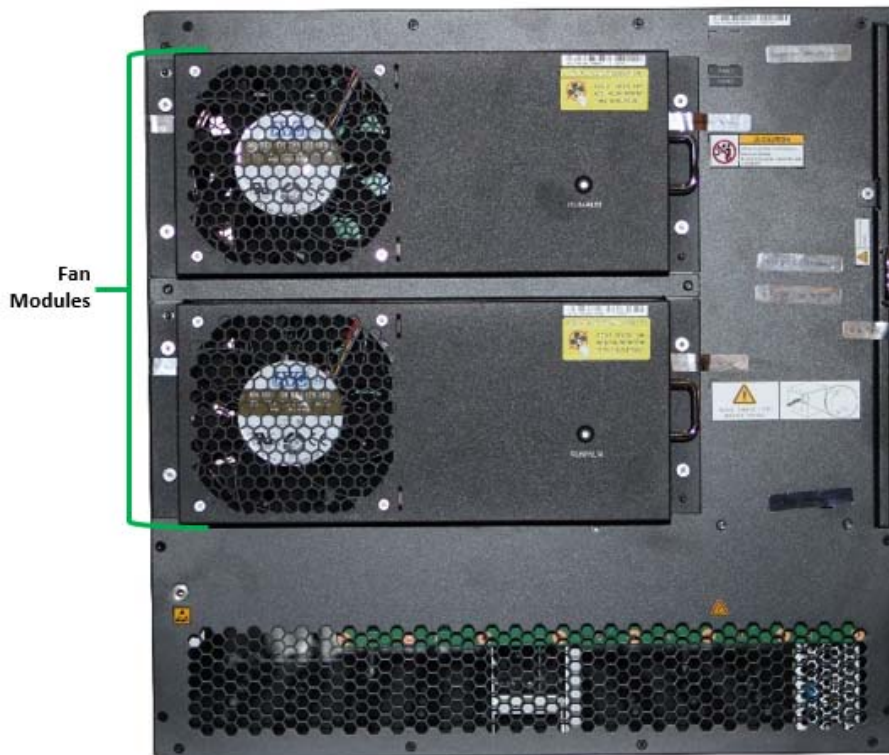


Figure 3-6: S7706 Ports – Back Panel

**Table 3-4: S7706 Module Ports and Interfaces**

Qty.	Port	Description	Logical Interface Type
2	MPU Card Slots	Main Processing Unit connection	Control in, data in, data out, status out. See Table 3-5.
2	CSS Card Slots (Sub Cards of MPU)	Network traffic	Control in, data in, data out, status out
6	LPU Card Slots <sup>2</sup>	Network traffic	Control in, data in, data out, status out. See Table 3-2.
8	Power Module Slots	Power	Power
2	Monitor Card Slots	Device Status	Status Out
2	Fan Module	Fan slot	N/A

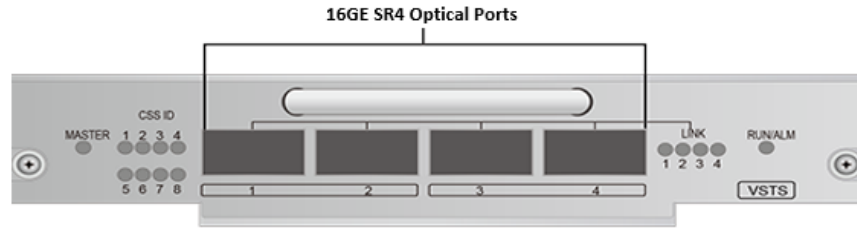
The FIPS validated configuration for the S7706 model includes two Main Processing Unit (MPU) Cards with the following ports and interfaces:

**Figure 3-7: S7706 MPU Card****Table 3-5: S7706 MPU Card Ports and Interfaces Mapping**

Port	Description	Logical Interface Type
Console	Serial console via RJ45 & miniUSB	Control in, data in, data out, status out
ETH management port	Management Ethernet interface	Control in, data in, data out, status out
LEDs	ACT, Run/ALM, Eth LEDs	Status out
RST Button	Reset the card	Control in

The FIPS validated configuration for the S7706 model includes two Content Services Switch (CSS) Cards with the following ports and interfaces:

<sup>2</sup> In the FIPS configuration, 1 LPU card is installed and the rest of the slots are covered with a faceplate.



**Figure 3-8: S7706 CSS Sub Card**

**Table 3-6: S7706 CSS Sub Card Ports and Interfaces Mapping**

Port	Description	Logical Interface Type
16GE SR4 optical ports (Qty. 4)	Network traffic	Control in, data in, data out, status out
LEDs	Run/ALM, CSS ID, LINK and Master LEDs	Status out



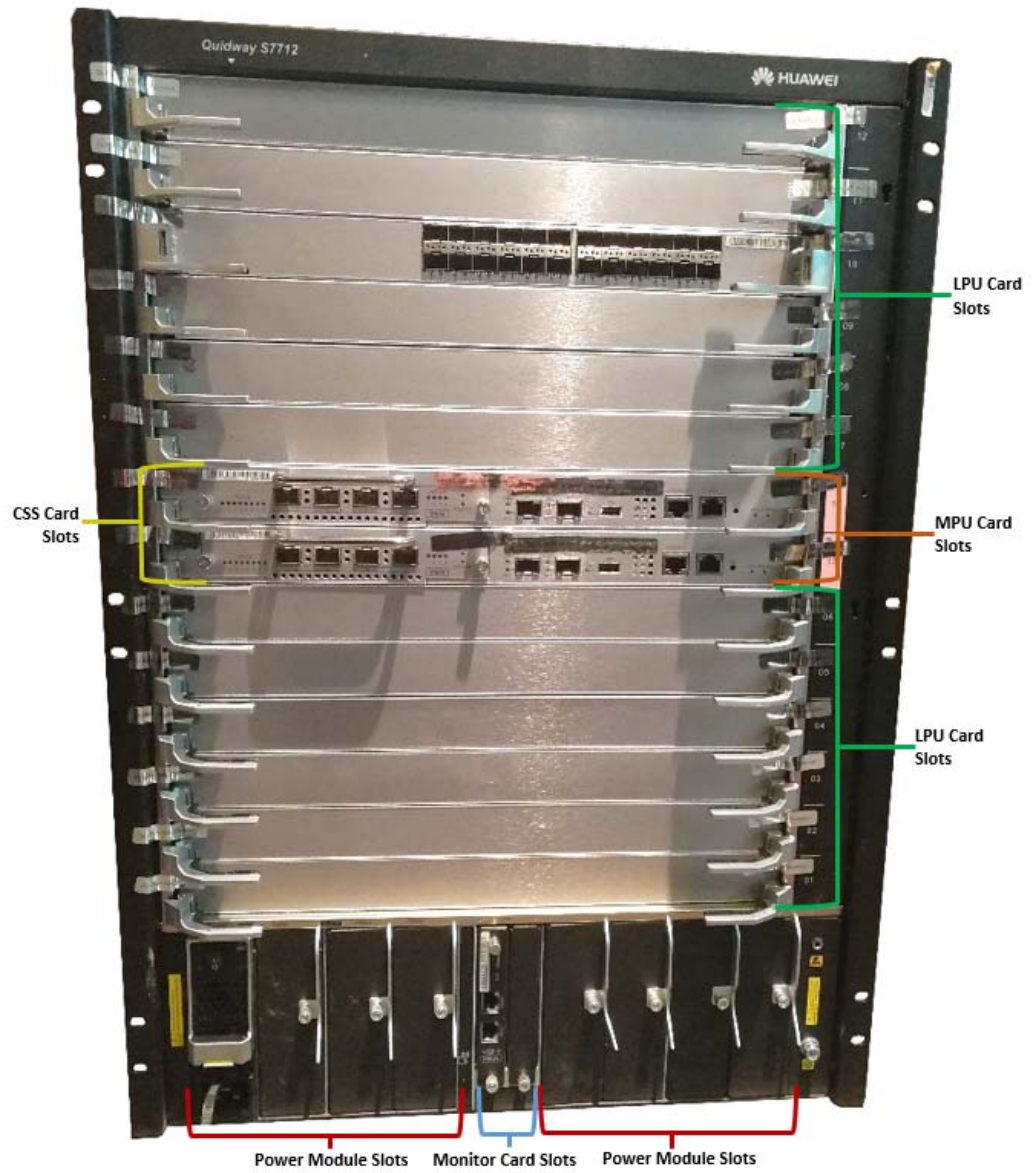
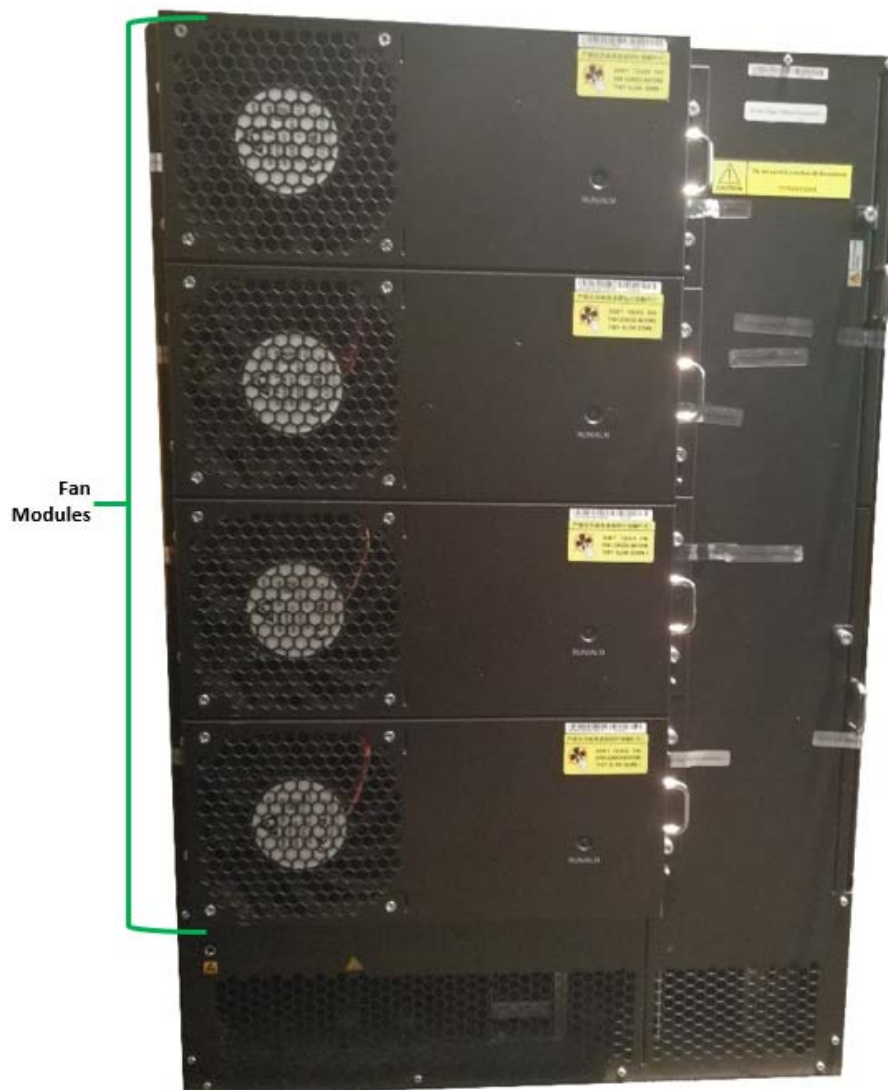


Figure 3-5: S7712 Ports – Front Panel



**Figure 3-6: S7712 Ports – Back Panel**

**Table 3-7: S7712 Module Ports and Interfaces**

Qty.	Port	Description	Logical Interface Type
2	MPU Card Slots	Main Processing Unit connection	Control in, data in, data out, status out. See Table 3-8.
2	CSS Card Slots (Sub Cards of MPU)	Network traffic	Control in, data in, data out, status out
12	LPU Card Slots <sup>3</sup>	Network traffic	Control in, data in, data out, status out. See Table 3-2.
8	Power Module Slots	Power	Power
2	Monitor Card Slots	Device Status	Status Out
4	Fan Module	Fan slot	N/A

<sup>3</sup> In the FIPS configuration, 1 LPU card is installed and the rest of the slots are covered with a faceplate.



The FIPS validated configuration for the S7712 model includes two Main Processing Unit (MPUs) Cards with the following ports and interfaces:

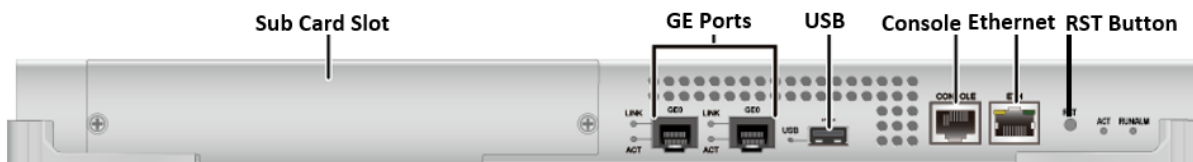


Figure 3-9: S7712 MPU Card

Table 3-8: S7712 MPU Card Ports and Interfaces Mapping

Port	Description	Logical Interface Type
GE ports (Qty. 2)	Reserved	N/A
USB	USB interface	Control in, data in, data out, status out
Console	Serial console via RJ45 & miniUSB	Control in, data in, data out, status out
ETH management port	Management Ethernet interface	Control in, data in, data out, status out
LEDs	ACT, Run/ALM, Eth, LINK, USB LEDs	Status out
RST Button	Reset the card	Control in

The FIPS validated configuration for the S7712 model includes two Content Services Switch (CSS) Cards with the following ports and interfaces:

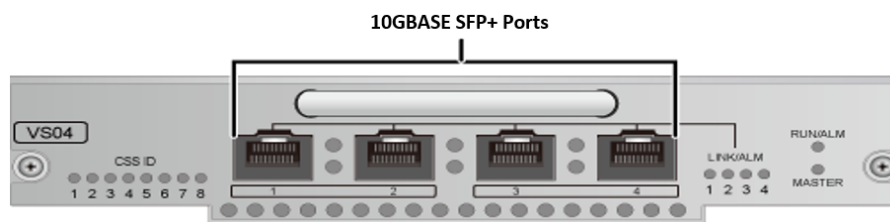


Figure 3-10: S7712 CSS Sub Card

Table 3-9: 7712 CSS Sub Card Ports and Interfaces Mapping

Port	Description	Logical Interface Type
10GBASE SFP+ ports (Qty. 4)	Network traffic	Control in, data in, data out, status out
LEDs	Run/ALM, CSS ID, LINK/ALM and Master LEDs	Status out

## 4 Cryptographic Functionality

The cryptographic protocols and primitives implemented and used by the modules are listed in this section. Table 4-1 and Table 4-2 list the TLS ciphersuites available in the Approved and non-Approved modes, respectively. Table 4-3 lists the SSH security methods; unlike TLS ciphersuites, SSH methods are independently selectable and may be used in any combination.

The module supports both an Approved and non-Approved mode of operation. By default, the module comes configured in the non-Approved mode. In the Approved mode, only the services listed in Tables 5-2 and 5-3 are available; further, the SSHv2 service is constrained to use only the Approved SSH options listed in Table 4-3. In the non-approved mode, all services in Tables 5-2, 5-3 and 5-4 are available for use, and all SSH options from Tables 4-3 are available.

The module supports https using TLS ciphersuites below in the Approved mode, supporting TLS to redirect all http connections to https (with TLS) and FTP to FTPS (with TLS) and to assure that a user cannot accidentally downgrade browser security.

**Table 4-1: TLS Ciphersuites used in the Approved mode**

Cipher Suite String (OpenSSL enumeration)	TLS	KX	AU	Cipher	Digest
TLS_RSA_WITH_AES_256_SHA	1.1, 1.2	RSA	RSA	AES-256	SHA-1, SHA-2
TLS_RSA_WITH_AES_128_SHA	1.1, 1.2	RSA	RSA	AES-128	SHA-1, SHA-2
TLS_DHE_RSA_WITH_AES_256_SHA	1.1, 1.2	DH	RSA	AES-256	SHA-1, SHA-2
TLS_DHE_DSS_WITH_AES_256_SHA	1.1, 1.2	DH	DSA	AES-256	SHA-1, SHA-2
TLS_DHE_RSA_WITH_AES_128_SHA	1.1, 1.2	DH	RSA	AES-128	SHA-1, SHA-2
TLS_DHE_DSS_WITH_AES_128_SHA	1.1, 1.2	DH	DSA	AES-128	SHA-1, SHA-2
TLS_RSA_AES_256_CBC_SHA256	1.2	RSA	RSA	AES-256	SHA-2

**Table 4-2: TLS Ciphersuites used in the Non-Approved mode**

Cipher Suite String (OpenSSL enumeration)	TLS	KX	AU	Cipher	Digest
TLS_RSA_WITH_DES_CBC_SHA	1.0, 1.1, 1.2	RSA	RSA	DES	SHA-1
TLS_RSA_WITH_RC4_128_MD5	1.2	RSA	RSA	RC4	MD5
TLS_RSA_WITH_RC4_128_SHA	1.2	RSA	RSA	RC4	SHA-1
TLS_RSA_WITH_NULL_MD5	1.0	RSA	RSA	NULL	MD5
TLS_RSA_WITH_NULL_SHA	1.0	RSA	RSA	NULL	SHA-1
TLS_DHE_RSA_WITH_DES_CBC_SHA	1.2	DH	RSA	DES	SHA-1

Cipher Suite String (OpenSSL enumeration)	TLS	KX	AU	Cipher	Digest
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	1.2	DH (2048)	DSA	Triple-DES	SHA-1
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	1.2	DH (2048)	DSA	AES-128	SHA-256
TLS_DHE_DSS_WITH_AES_128_CBC_SHA	1.0, 1.1, 1.2	DH (2048)	DSA	AES-256	SHA-1
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	1.2	DH	DSA	AES-256	SHA-256
TLS_DHE_DSS_WITH_AES_256_CBC_SHA	1.0, 1.1, 1.2	DH	DSA	AES-256	SHA-1
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	1.2	DH	DSA	AES-128	SHA-256
TLS1_CK_RSA_RC4_128_SHA	1.1,1.2	RSA	RSA	AES-256	SHA-1

The module uses SSHv2 over a shell interface via the console serial port to perform module configuration and administration.

**Table 4-3: SSH Security Methods Available in Each Mode**

SSH Security Methods	Approved Mode	Non-Approved Mode
<b>Key Exchange</b>		
diffie-hellman-group14-sha1	X	X
diffie-hellman-group-exchange-sha1	X	X
<b>Server Host Key (Authentication)</b>		
ssh-dss	X	X
ssh-rsa	X	X
ssh-ecdsa	X	X
<b>Digest</b>		
hmac-md5-96		X
hmac-md5-128		X
hmac-sha1	X	X
hmac-sha1-96	X	X
hmac-sha2-128	X	X
Hmac-sha256	X	X
<b>Cipher</b>		
des-cbc		X
aes128-ctr		X
aes-256-ctr		X
aes-128-cbc	X	
aes-256-cbc	X	X
3des-cbc	X	X

In the non-Approved mode, the module supports SSH v1.5 with the same set of algorithms listed above.

Table 4-4, Table 4-5 and Table 4-6 list all Approved, Allowed and non-Approved algorithms used by the library, respectively.

**Table 4-4: Approved Algorithms**

CAVP Cert. #	Algorithm	Standard	Mode/Method	Strength <sup>4</sup>	Use
Library: HFCL					
4400	AES	FIPS 197, SP 800-38A	CBC	128 or 256	Data encryption/decryption
Vendor affirmed	CKG	SP 800-133	N/A	N/A	Key generation
1107 (CVL)	TLS <sup>5</sup> KDF	SP 800-135	1.0/1.1 (SHA-1) 1.2 (SHA-256)		KDF used to derive TLS session keys
	SSH <sup>2</sup> KDF	SP 800-135	SHA-1, SHA-256, SHA-384, SHA-512		KDF used to derive SSH v2 session keys
1418	DRBG <sup>6</sup>	SP 800-90A	Hash_DRBG	256	Deterministic random bit generation
1175	DSA	FIPS 186-4	Mod 2048 Mod 2048 (SHA-1; for protocol use only) Mod 2048 (SHA-1/256)		Key generation Signature generation Signature verification
1057	ECDSA	FIPS 186-4	P-256, P-384, P-521 P-256, P-384, P-521 (SHA-2) P-256, P-384, P-521 (SHA-2)		Key generation Signature generation Signature verification
2924	HMAC	FIPS 198-1	HMAC-SHA-1 HMAC-SHA-256	128 256	Message authentication
(based on 2924)	HMAC	IG A.8	HMAC-SHA-1-96 HMAC-SHA-256-128		Message authentication in SSH
4400 2924	KTS: AES HMAC	SP 800-38F	Key Wrap	128 or 256	Key establishment
2372 2924	KTS: Triple-DES HMAC	SP 800-38F	Key Wrap	112	Key establishment
2380	RSA	FIPS 186-4	Mod 2048 Mod 2048 (SHA-1/256; SHA-1 for protocol use only) Mod 2048 (SHA-1/256)		Key generation Signature generation Signature verification
3627	SHS	FIPS 180-4	SHA-1 SHA-2: SHA-256/384/512		Message digest generation
2372	Triple-DES	SP 800-67	TCBC	3-Key	Data encryption/decryption

<sup>4</sup> Strength indicates DRBG Strength, Key Lengths, Curves or Moduli

<sup>5</sup> The TLS and SSH protocols have not been reviewed or tested by the CAVP and CMVP

<sup>6</sup> No prediction resistance; hash\_df used for instantiation.

**Table 4-5: Allowed Algorithms**

Algorithm	(Establishment) Strength	Use
Diffie-Hellman Key Agreement	DH Group 14 (2048-bit modulus) (key establishment methodology provides 112 bits of encryption strength).	Key establishment.
MD5	No strength claimed.	TLS 1.0/1.1 password hash.
NDRNG	Internal entropy source with rationale to support the claimed DRBG security strength.	DRBG (Cert. #1418) entropy input.
RSA Key Wrapping	2048-bit modulus (key establishment methodology provides 112 bits of encryption strength).	Key establishment.

**Table 4-6: Non-Approved Algorithms (Used only in the non-Approved Mode)**

Algorithm	Use
AES-XCBC-MAC	Data encryption/decryption
AES CTR (non-compliant)	Data encryption/decryption
DES	Data Encryption/Decryption
Diffie-Hellman	DH Group 1 (768-bit modulus): Key exchange within SSH
HMAC-MD5	Message Digest Generation
MD5	Message Digest Generation
RC4	TLS encryption
RSA (non-compliant)	512 or 1024 bit key sizes for signature generation
Triple-DES (non-compliant)	2-key for data encryption/decryption.
SNMP KDF (non-compliant)	KDF used to derive SNMP keys. <sup>7</sup>

---

<sup>7</sup> Keys derived from the SNMP protocol cannot be used in the Approved mode.

## 4.1 Critical Security Parameters and Public Keys

All CSPs used by the module are described in this section.

**Table 4-7: Critical Security Parameters (CSPs)**

Name	Description and usage
AUTH-PW	Authentication Passwords, minimum of 8 characters
DRBG-EI	Entropy input (1024 bytes) to the hash_df used to instantiate the Approved Hash_DRBG.
DRBG-STATE	SP 800-90A Hash_DRBG V and C values (SHA-256, 440-bit V, per IG 14.5).
SSH-DH	SSH Diffie-Hellman private component (2048-bit). Ephemeral DH private key used in SSH.
SSH-Priv	SSH private key. RSA (2048), DSA (2048), or ECDSA private key used to establish SSH sessions.
SSH-SENC	SSH Session Encryption Key. AES-128, AES-256 or 3-Key Triple-DES key for SSH message encrypt/decrypt.
SSH-SMAC	SSH Session Authentication Key. HMAC-SHA 160-bit session key for SSH message authentication.
TLS-Host-Priv	TLS private key. RSA (2048) or DSA (2048) private key used to establish TLS sessions.
TLS-DH-Priv	TLS Diffie-Hellman private component (2048-bit). Ephemeral DH private key used in TLS.
TLS-PMS	TLS pre-master secret (size dependent on the key exchange method) used to derive TLS-SENC and TLS-SMAC.
TLS-SENC	TLS Session Encryption Keys. AES-128, AES-256 or 3-Key Triple-DES key for TLS message encrypt/decrypt.
TLS-SMAC	TLS Session Authentication Keys. HMAC-SHA-1 (160-bit) or HMAC-SHA-256 (256-bit) session key for TLS message authentication.

**Table 4-8: Public Keys**

Name	Description and usage
SSH-Peer-Pub	SSH public key. RSA (2048) or DSA (2048) public key used for SSH client authentication.
SSH-Pub	SSH public key. RSA (2048) or DSA (2048) public key used for SSH session establishment.
SSH-DH-Pub	SSH Diffie-Hellman public component (2048 bit). Ephemeral DH public key used in SSH.
TLS-Host-Pub	TLS public key. RSA (2048) or DSA (2048) public key used for TLS session establishment.
TLS-DH-Pub	TLS Diffie-Hellman public component (2048 bit). Ephemeral DH public key used in TLS.
FW-Update-Pub	RSA (2048) public key used to verify firmware updates.

## 5 Roles, Authentication and Services

### 5.1 Assumption of Roles

The module does not support a maintenance role or bypass capability. The module supports concurrent use by End Users and Administrators. The cryptographic module enforces the separation of roles by the partitioning of major subsystems (such as end user traffic vs. shell or administrative functions), and by partitioning of the administrative interfaces (e.g. by organization of the web GUI pages). Authentication status does not persist across module power cycles. To change roles, an operator must first log out, then log in using another role.

Table 5-1 lists the available roles; the options for authentication type and data are common across roles.

**Table 5-1: Roles Description**

Role		Authentication	
ID	Description	Type	Data
Management User (CO)	Cryptographic Officer – Has full access to administer and configure the module as well as delegate admin access control rights to Administrators.	Identity-based (using <i>Local password verification</i> or <i>digital signature verification</i> )	Username and Password or X.509 certificate
Monitoring User (MU)	Accesses audit logs for diagnostic information		
End User (EU)	Typical end user switch network traffic.		

### 5.2 Authentication Methods

The *Local password verification* method requires an 8 character minimum password using characters from at least two categories of printable character sets (upper case, lower case, special character, and numbers).

Since there are 28 possible special characters, 10 number characters and 26 upper or lower case characters, the weakest password that meets the policy but whose components are still chosen randomly would be 7 digits and one upper or lower case character. This results in an upper bound probability of  $(10^7) \times 26$ . So, the probability of guessing the password with a single attempt is  $1/(2.6 \times 10^8)$  which is less than one in 1,000,000.

For SSH connections, after  $n$  consecutive unsuccessful authentication attempts, the module will lockout additional authentication requests for a minimum of 5 minutes. The default value for  $n$  is 3, but per the security rules must be less than 2600.

The probability of false authentication in a one minute period is  $2599/(2.6 \times 10^8) = 1/100038$ .

For console access, after 1 unsuccessful attempt, the module requires a waiting period of 5 seconds before accepting another authentication attempt. Thus, only 12 authentication attempts are possible over the console in a one minute period.

The probability of a false authentication in a one minute period is  $12/(2.6 \times 10^8)$ , which is less than 1 in 100,000.

The *digital signature verification* method, used for SSH client-side authentication, is based on the verification of a 2048-bit RSA or DSA digital signature, which has a minimum equivalent computational resistance to attack of  $2^{112}$ .

The probability of a successful random attempt is  $1/(2^{112})$ , which is less than 1/1,000,000.

Processing speed limits the number of failed authentication attempts in a one-minute period to 120 attempts.

The probability of a success with multiple consecutive attempts in a one-minute period is  $120/(2^{112})$ , which is less than 1/100,000.

## 5.3 Services

All services implemented by the module are summarized next, with additional detail in Table 5-5 provided for traceability of cryptographic functionality and access to CSPs and public keys by services.

**Table 5-2: Authenticated Module Services**

Service	Description	CO	MU	EU
Module Reset	Reboot the module via reset CLI command or WebGUI. This service executes the suite of self-tests required by FIPS 140-2.	X	X	
Reset to Factory	Resets to factory defaults by deleting the module's configuration file and rebooting the system.	X	X	
Configure System (includes Firmware Update)	Update module firmware, module configuration, file management, and logging configuration.	X	X	
Configure Network	Network Interface configuration and management.	X	X	
Status Monitoring and Reporting	Including Monitor and Dashboard GUI, provides module status (CPU usage, etc.) and logs.	X	X	
User Management and Authentication	Creating users and setting access rights.	X	X <sup>8</sup>	
SSHv2	Configure SSH v2 parameter, provide entry of CSPs.	X		
HTTPS	HTTP over TLS 1.1/1.2	X		

<sup>8</sup> Only Management Users with a user level set between 3 and 15 can manage other administrator accounts



Service	Description	CO	MU	EU
Switched network traffic	Provide service through L2TP, GRE and MPLS.			X

(Note: This is a condensed list of services for the purposes of this Security Policy. The full list of module commands can be found in the module's User manual. The link to the User Manual is provided below in Section 10).

**Table 5-3: Unauthenticated Module Services**

Service	Description
Power-up Self-tests	This service executes the suite of self-tests required by FIPS 140-2 by power cycling the module.
Switched Network Traffic Management	DHCP, DNS, traffic routing, NTP, NAT network traffic.
Show Status	This service provides the current status of the cryptographic module via LEDs and other unauthenticated status outputs.

**Table 5-4: Services only available in Non-FIPS mode**

Service	Description
Remote AAA	Connection to remote AAA server (RADIUS, TACACS)
SNMP v1/v2/v3	Configuration, administration and monitoring
FTP	File upload and download
TFTP	File upload and download
SSHv1.5	Config and Manage device over SSH
HTTP	Config and Manage device through WebGUI
Telnet	Using telnet to remotely manage and maintain several devices without the need to connect each device to a terminal, data is transmitted using TCP in plaintext.

Table 5-5 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as:

G = Generate: The module generates the CSP.

R = Read: The module reads the CSP. The read access is typically performed before the module uses the CSP.

E = Execute: The module executes using the CSP.

W = Write: The module writes the CSP. The write access is typically performed after a CSP is imported into the module, when the module generates a CSP, or when the module overwrites an existing CSP.

Z = Zeroize: The module zeroizes the CSP.

Table 5-5: CSP/Public Key Access Rights within Services

Services	AUTH-PW	DRBG-EI	DRBG-STATE	SSH-DH	SSH-Priv	SSH-SENC	SSH-SMAC	TLS-Host-Priv	TLS-DH-Priv	TLS-PMS	TLS-SENC	TLS-SMAC	SSH-Peer-Pub	SSH-Pub	SSH-DH-Pub	TLS-Host-Pub	TLS-DH-Pub	FW-Update-Pub
Unauthenticated																		
Power-up Self-tests	--	GE	G	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Switched Network Traffic Management	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Show Status	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Management User (CO)																		
Module Reset	--	GE	G	--	--	Z	Z	--	--	Z	Z	Z	--	--	--	--	--	--
Reset to Factory	Z	GE Z	GZ	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	--
Configure System	E	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Configure Network	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Status Monitoring and Reporting	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
User Management and Authentication	R W Z	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
SSHv2	--	G RE	G RE	G RE W	G RE W	G RE W	G RE W	--	--	--	--	--	RE	G RE	G RE W Z	--	--	--
HTTPS	--	G RE	G RE	--	--	--	--	RE W	RE W	RE W	RE W	RE W	--	--	--	RE	RE	RE W
Monitoring User (MU)																		
Module Reset	--	GE	G	--	--	Z	Z	--	--	Z	Z	Z	--	--	--	--	--	--
Reset to Factory	Z	GE Z	GZ	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	--
Configure System	E	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Configure Network	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Status Monitoring and Reporting	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
User Management and Authentication	R W Z	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
End User (EU)																		
Switched Network Traffic	E	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

The Module Reset service instantiates the DRBG, with 1024 bytes of entropy input (DRBG-EI) produced by the Allowed NDRNG. The generation of DRBG-State uses the [SP 800-90A] Hash\_df with 660 bits of entropy input. Internally generated symmetric keys are the result of unmodified output from the DRBG. The zeroization of session keys by this service covers the case of module shutdown or power-cycle while a secure channels session (SSH, TLS) is active.

The Show Status service does not access CSPs or public keys.

## 6 Self-tests

Each time the module is powered up it tests that the cryptographic algorithms still operate correctly and that sensitive data have not been damaged. Power up self-tests are available on demand by power cycling the module.

On power up or reset, the module performs the self tests described in below. All KATs must be completed successfully prior to any other use of cryptography by the module. Once called, the initialization function does not allow any user intervention.

All data output via the data output interface is inhibited when an error state exists and during self-tests. Upon successful completion of the self-tests the modules SYS LED will go from Red to Green. If a failure of a self-test occurs, the module enters an error state, outputs the following error message on the console and forces the module to reboot: "Self-Test Fail..."

**Table 6-1: Power Up Self-tests**

Test Target (Cert. #)	Description
Firmware Integrity	32 bit CRC performed over all code
AES (#4400)	Separate encrypt, decrypt KATs using 128 and 256 bit keys and CBC.
Diffie Hellman	Shared secret calculation KAT
DRBG (#1418)	SHA-256 Hash DRBG test. Performed conditionally (where initial use at power-up is the condition) per SP 800-90A Section 11.
DSA (#1175)	Pairwise consistency test of n=2048 bit signature generation and signature verification.
ECDSA (#1057)	Pairwise consistency test of P-256 signature generation and signature verification.
HMAC (#2924)	Separate HMAC generation and verification KATs, using SHA-1, SHA-256
RSA (#2380)	Separate KATs of n=2048 bit signature generation and signature verification.
SHS (#3627)	Separate KAT of SHA-1, SHA-256, SHA-384, SHA-512
Triple-DES (#2372)	Separate encrypt, decrypt KATs using 3-key TCBC (192 bits).

**Table 6-2: Conditional Self-tests**

Test Target	Description
NDRNG	AS09.42 Continuous RNG Test performed on each NDRNG access.
DRBG	AS09.42 Continuous RNG Test performed on each DRBG access.
ECDSA	Pairwise Consistency Test performed on each ECDSA key pair generation
DSA	Pairwise Consistency Test performed on each DSA key pair generation
RSA	Pairwise Consistency Test performed on each RSA key pair generation.
Firmware Load	RSA 2048 and SHA-256 signature verification performed by the firmware load service.

## 7 Physical Security Policy

The cryptographic modules each include the following physical security mechanisms:

- Production-grade components and production-grade opaque enclosure
- Tamper-evident material and seals

An operator in the CO role is responsible for the following:

- Applying the tamper seals per Section 7.1 below. The tamper evident seals shall be installed for the module to operate in a FIPS Approved mode of operation. The CO is responsible for having control at all times of any unused seals.
- Inspecting the tamper seals based on the schedule described in Table 7-1 below.

**Table 7-1: Physical Security Inspection Guidelines**

Mechanism	Recommended Frequency of Inspection/Test
Tamper-evident Seals	Inspect tamper-evident seals monthly. If evidence of tamper exists, the CO should zeroize the module immediately and reapply tamper-evident seals.

### 7.1 Tamper Seal Placement

#### 7.1.1 S7703

The module includes 11 tamper-evident seals, which are applied as follows:

- 8 seals applied to the front frame and each card or card plate, preventing removal of individual components and cover plates (see #1 to #8 in Figure 7-1)
- 2 seals applied to the back and fan covers (see #9 & #10 in Figure 7-1 and Figure 7-3)
- 1 seal applied to the back and ventilation air filter (see #11 in Figure 7-2)



**Figure 7-1: Tamper Seal Locations - Front**



**Figure 7-2: Tamper Seal Locations - Back**



**Figure 7-3: Tamper Seal Location - Right Side**

## 7.1.2 S7706

The module includes 27 tamper-evident seals, which are applied as follows:

- 16 seals applied to the front frame and each card or card plate, preventing removal of individual components and cover plates (see #1 to #16 in Figure 7-4)
- 2 seals applied to the front center card, preventing removal (see #17 to #18 in Figure 7-4)
- 4 seals applied to the back and fan covers (see #19 to #22 in Figure 7-5, and #19 and #21 in Figure 7-6)
- 4 seals applied to the back, covering holes (see #23 to #26 in Figure 7-5)
- 1 seal applied to the back and ventilation air filter (see #27 in Figure 7-5)



Figure 7-4: Tamper Seal Locations - Front

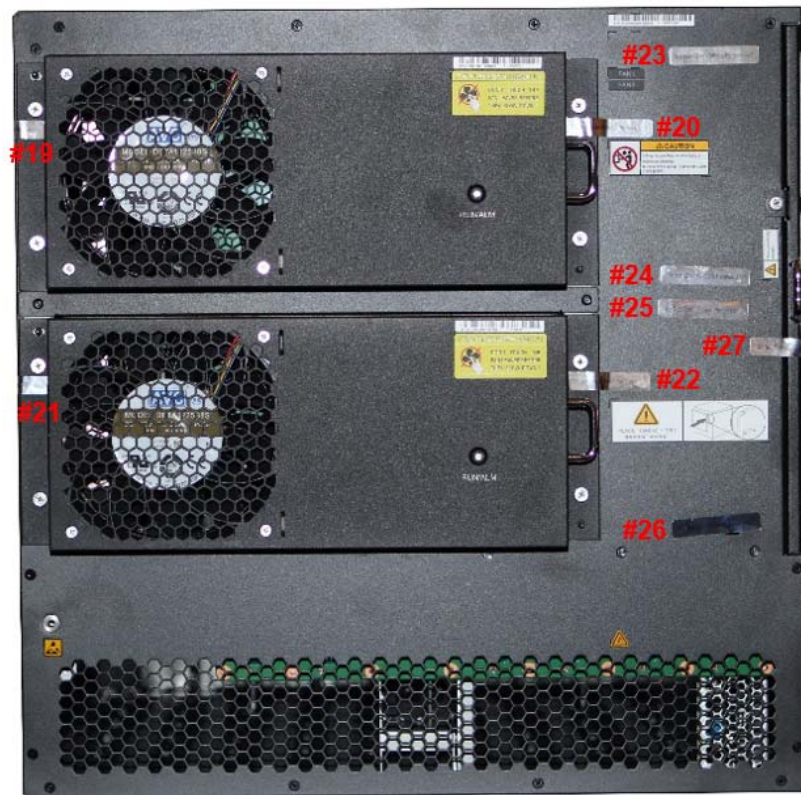


Figure 7-5: Tamper Seal Locations – Back



**Figure 7-6: Tamper Seal Locations - Right Side**

### 7.1.3 S7712

The module includes 48 tamper-evident seals, which are applied to the module as follows:

- 28 seals applied to the front frame and each card or card plate, preventing removal of individual components and cover plates (see #1 to #28 in Figure 7-7)
- 2 seals applied to the front center card, preventing removal (see #29 to #30 in Figure 7-7)
- 4 seals applied to the front center card ventilation, obstructing view (see #31 to #34 in Figure 7-7)
- 8 seals applied to the back and fan covers (see #35 to #42 in Figure 7-8, and #35, #37, #39 and #41 in Figure 7-9)
- 4 seals applied to the back, covering holes (see #43 to #46 in Figure 7-8)
- 2 seals applied to the back and ventilation air filter (see #47 and #48 in Figure 7-8)



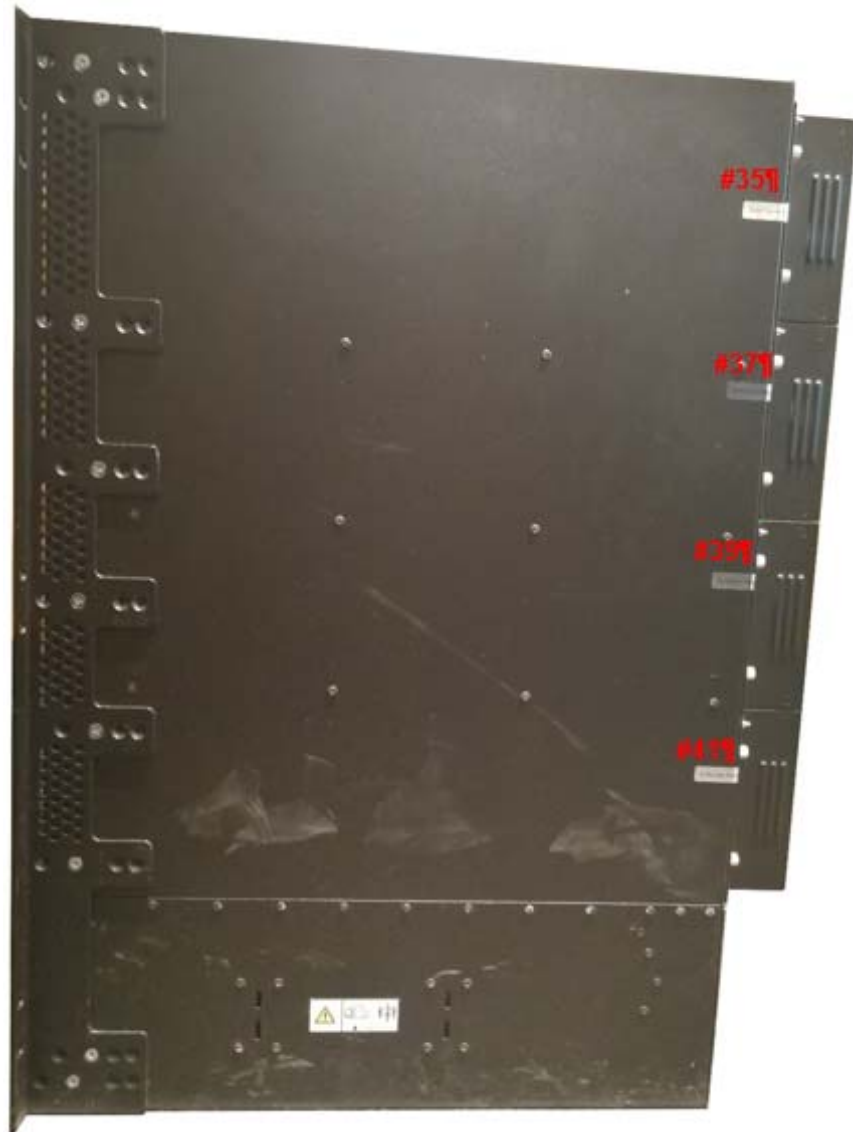


Figure 7-7: Tamper Seal Locations - Front





Figure 7-8: Tamper Seal Locations – Back



**Figure 7-9: Tamper Seal Locations - Right Side**

## 8 Operational Environment

---

The module is designated as a limited operational environment under the FIPS 140-2 definitions.

## 9 Mitigation of Other Attacks Policy

---

The modules have not been designed to mitigate attacks outside the scope of FIPS 140-2.

## 10 Security Rules and Guidance

---

The module design corresponds to the module security rules. The module implements and enforces the following security rules:

1. An unauthenticated operator does not have access to any CSPs or cryptographic services.
2. The module inhibits data output during power up self-tests and error states.
3. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
4. Zeroization overwrites all CSPs.
5. The module does not share CSPs between the Approved mode of operation and the non-Approved mode of operation.

The following security rules must be adhered to for operation in the FIPS 140-2 Approved mode:

6. Upon first time initialization, the Root Administrator (CO) shall authenticate to the module using the default username and password:

Username: admin

Password: Admin@huawei

7. Set the workmode to FIPS:

The following CLI command initiates the steps for placing the controller in FIPS approved mode of operations, and enabling all necessary algorithm restrictions. All necessary self-tests are carried out in both FIPS and non-FIPS modes.

```
[quidway]set work-mode fips
```

**Warning: The work mode of device will change and system will restart. Continue?**  
[Y/N]: y

After completing the steps, saving the configuration and rebooting, the Controller stays in FIPS mode unless the FIPS mode is explicitly disabled. The non-approved cryptographic algorithms do not get used in FIPS mode unless they are explicitly configured.

To view the current mode of operation, the following CLI command needs to be used:

```
[quidway]display work-mode
```

**Work mode : FIPS**

Upon the reboot the CO shall update from the default username and password. The minimum password strength is enforced by the module per Section 3.2. The CO can then create Administrator and End User accounts and proceed with module configuration per the vendor provided user manual (available here: <http://http://support.huawei.com/enterprise/en/switch/s7700-pid-6805481>).

A crypto officer can use the following CLI command to set user passwords:

```
[quidway-aaa]local-user user-name password irreversible-cipher password
```

```
[quidway-aaa]local-user user-name service-type https/ssh
```

```
[quidway-aaa]local-user user-name privilege level 15
```

```
[quidway-aaa]local-aaa-user password policy administrator (optional)
```

Note that this and all subsequent configuration steps may also be performed through HTTPS. However, only the CLI commands are included in this document.

8. Configure SSH using the following:

```
[quidway]ssh user user-name
[quidway] ssh user user-name authentication-type { password | rsa | password-rsa | all |
dsa | password-dsa }
[quidway] ssh user username service-type stelnet / sftp
[quidway] rsa local-key-pair create, or dsa local-key-pair create.
[quidway] ssh server key-exchange dh_group_exchange_sha1
```

#### 9. Configure an HTTPS Certificate

The following commands configure the web server to use the manufacturer-installed switch device certificate for the HTTPS server. It must be executed after enabling FIPS mode of operation:

```
[quidway] ssl policy policy-name
```

Load a PEM certificate or certificate chain. Run either of the following commands based on whether a user obtains a digital certificate or certificate chain from the CA.

```
[quidway] certificate load pem-cert cert-filename key-pair { dsa | rsa } key-file key-
filename auth-code cipher auth-code
```

A PEM digital certificate is loaded and the private key file is specified.

Or:

```
[quidway] certificate load pem-chain cert-filename key-pair { dsa | rsa } key-file key-
filename auth-code cipher auth-code
```

A PEM certificate chain is loaded and the private key file is specified.

```
[quidway] certificate load asn1-cert cert-filename key-pair { dsa | rsa } key-file key-
filename
```

An ASN1 digital certificate is loaded and the private key file is specified.

```
[quidway] certificate load pfx-cert cert-filename key-pair { dsa | rsa } { mac cipher
mac-code | key-file key-filename } auth-code cipher auth-code
```

A PFX digital certificate is loaded and the private key file is specified.

```
[quidway] http secure-server ssl-policy policy-name
```

In non-FIPS mode, a self-signed certificate may be used for the HTTPS server.

#### 10. The CO must not configure the failed authentication limit setting for more than 2599.

#### 11. Save and Reboot

After executing the above commands, you must save the configuration and reboot the system:

```
<quidway> save
<quidway> reboot
```

An operator of the module can determine if the module is running the in Approved mode of operation by adhering to the above rules.