HUAWEI

HUAWEI OptiX OSN 1800 Series

Non-Proprietary FIPS 140-2 Security Policy

Document Version: 1.3

Date: April 28, 2021

Table of Contents

Change Record

Revision	Date	Author	Note
0.1	16/01/2019	LIJIA	Initial Draft
0.3	31/01/2019	ZHANGJIAN/CHENPENG	After workshop with UL
0.4	11/03/2019	ZHANGJIAN/CHENPENG	After workshop with UL
0.5	09/04/2019	LIXIANG	Change Picture
0.6	22/04/2019	ZHANGJIAN/CHENPENG	Amended as per UL comments
0.7	26/08/2019	ZHANGJIAN/CHENPENG	Recommended UL changes
1.0	22/11/2019	ZHANGJIAN/CHENPENG	Minor changes for publication
1.1	9/02/2021	ZHANGJIAN/CHENPENG	Changes as a result of CMVP comments
1.2	3/25/2021	ZHANGJIAN/CHENPENG	Changes as a result of CMVP comments
1.3	4/28/2021	ZHANGJIAN/CHENPENG	Changes as a result of CMVP comments

1. Introduction

HUAWEI OptiX OSN 1800 Series (OptiX OSN 1800 V and OptiX OSN 1800 IIE), hereafter denoted the OSN 1800 V/1800 IIE are applicable to the metro edge layers including the metro convergence layer and the metro access layer and it is generally deployed in the upstream of wired broadband and mobile carrier facilities. Services such as the broadband, Synchronous Digital Hierarchy (SDH), and Ethernet services are processed at the metro access layer and then sent to the convergence node on the metro transport network.

The module is a multi-chip standalone cryptographic module enclosed in hard, commercial grade metal cases. The cryptographic boundary for these modules is the entire enclosure. 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 non-modifiable 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.

The module will also be used in markets other than US Federal Agencies that require FIPS140-2.

Table 1 - Cryptographic Module Configuration

Module	HW P/N	FW Version
OSN1800 V	02300783	V100R009C00SPC300 5.67.09.16T26
OSN1800 IIE	02301163	V100R009C00SPC300 5.67.09.16T26

The major components that were tested with each module are listed in the tables below:

Table 2 - Major Components with OSN 1800 V

Name	Description	Part Number	Version
TNZ5UXCMS	System, Control and Communication Board	60:023GBW10J8004412 50:023GBW10H3000534	logic: (U1212) 530, (U1214) 300, (U1210) 130 The numbers outside the parenthesis are the FPGA or CPLD versions.
TNF1CE6	WDM Interface Board	022PYL10HC000078*	VER.A
TNF1LDCA	WDM Interface Board	032VFR10JA000121*	VER.B
TNF6TTA	Client-side Optical Interface Board	031YNU10GC000362	VER.B
TNZ5UNS4	WDM-side Optical Interface Board	032AUB10JA000039	VER.B

Name	Description	Part Number	Version
TNF6APIU	AC Power Supply	2102312ADY10J6000005 2102312ADY10J6000011	VER.B
TNF5PIU	DC Power Supply	021YNWD0K1001350 021YNWD0J8001151	VER.B
TNFK01AFB	Backplane Board	2102300783N0JB000695	VER.B
TNF5FAN	Fan	2102120877N0JB000647	VER.B
	Tamper-Evident Seal*	Y4697666*	N/A

Note: Two (2) different power configurations were tested:

1. Two (2) TNF6APIU AC Power Supplies
2. Two (2) TNF5PIU DC Power Supplies

Two (2) of the same kind of power supplies are required for redundancy.

Table 3 - Major Components with OSN 1800 IIE

Name	Description	Part Number	Version
TNZ2UXCL	System, Control and Communication Board	023VFQ10J8000390 023VFQ10J8000392	logic: (U40) 210, (U55) 120, (U48) 210, (U17) 100 The numbers outside the parenthesis are the FPGA or CPLD versions.
TNF1CE6	WDM Interface Board	022PYL10HC000078*	VER.A
TNF1LDCA	WDM Interface Board	032VFR10JA000121*	VER.B
TNZ1APIU	AC Power Supply	A1163190103002V0 A1163190103010V0	VER.A
ANK1PIU	DC Power Supply	023NKNLUJA010598 023NKNLUJA010621	VER.A
TNZ2K01AFB	Backplane Board	2102301163N0JB000002	VER.B
TNZ1FAN	Fan	032MUSN0JB000002	VER.A
	Tamper-Evident Seal*	Y4697666*	N/A

Note: Two (2) different power configurations were tested:

1. Two (2) TNZ1APIU AC Power Supplies
2. Two (2) ANK1PIU DC Power Supplies

Two (2) of the same kind of power supplies are required for redundancy.

*Are used in both modules

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

Table 4 - 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	2
Mitigation of Other Attacks	N/A
Overall	2

1.1 Module Description and Cryptographic Boundary

The physical forms of the Modules are depicted in Figure 1 and Figure 2. The Modules are multi-chip standalone embodiments. The cryptographic boundary for each module is indicated with a red outline.

Only the front panel is displayed for each module because the rear, top, bottom, and sides of the metal enclosure do not present any ports. The hard, grey, metal enclosure is called a subrack. The boards slide into the subrack and are held in place by screws.

Figure 1 - Cryptographic Boundary of OSN 1800V

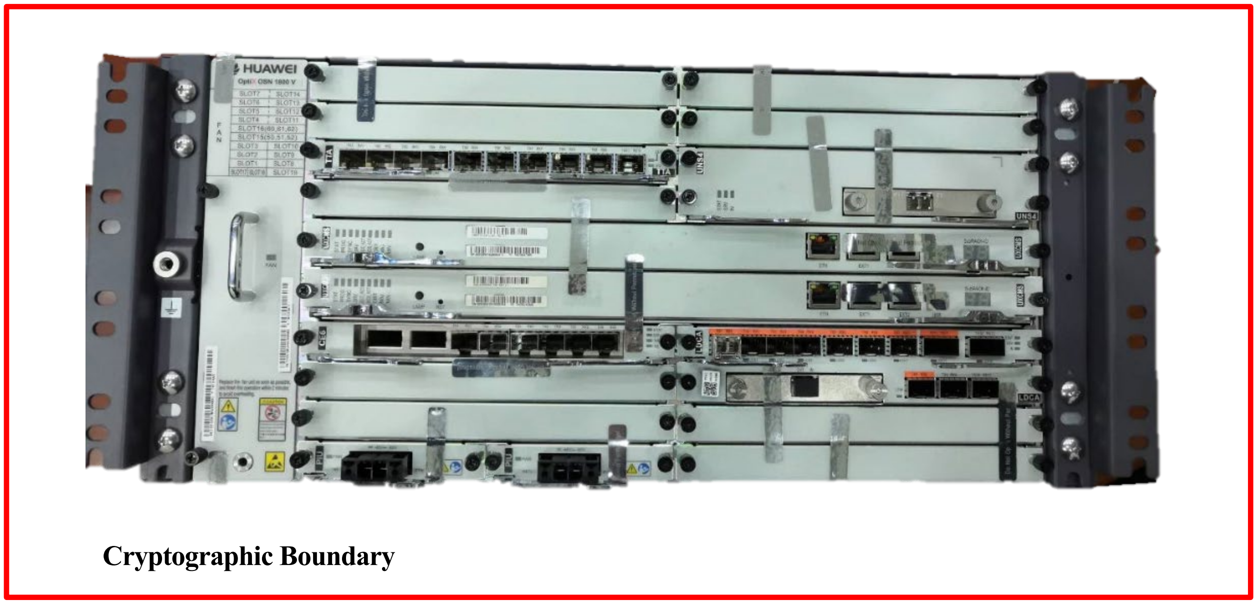
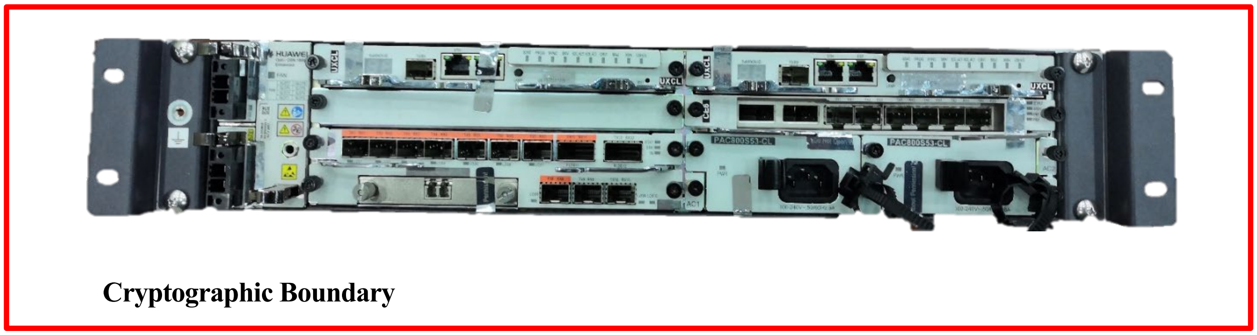


Figure 2 - Cryptographic Boundary of OSN 1800 IIE



The module's ports and associated FIPS defined logical interface categories are depicted in Figure 3 through Figure 14 and listed in Table 5 through Table 16.

Figure 3 - Physical Form of the Subrack (OSN1800 V)

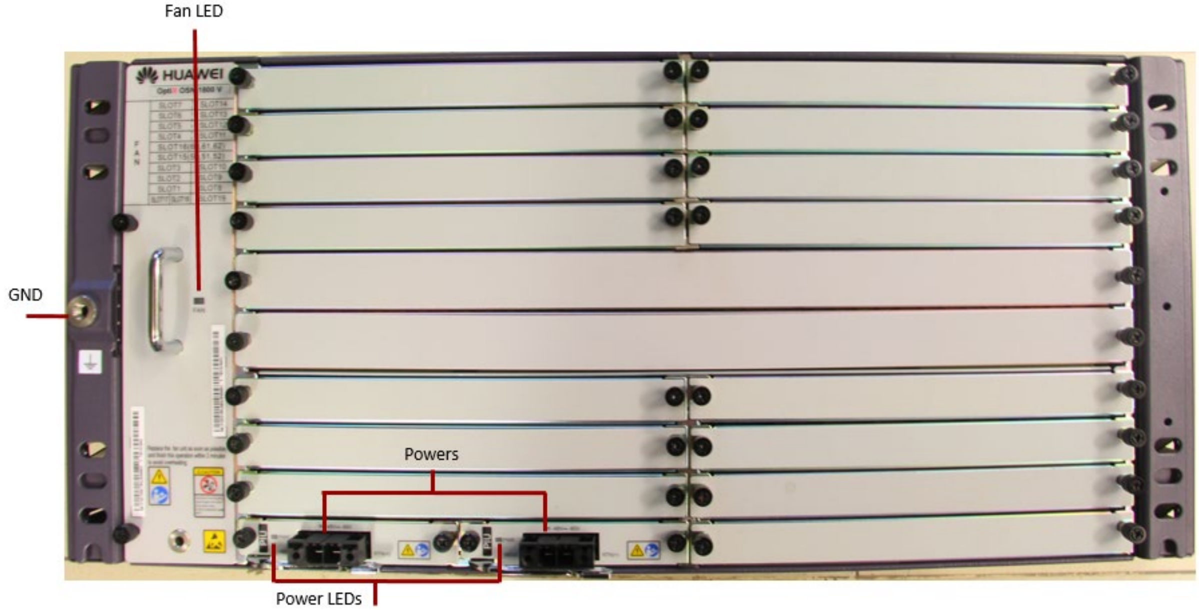


Table 5 - Ports and Interfaces on the Subrack (OSN1800 V)

Port	Description	Logical Interface Type
Fan LED	Fan status	Status out
Powers and GND	DC power supply	Power
Power LEDs	Power status	Status out

Figure 4 - Physical Form of the Subrack (OSN1800IIE)

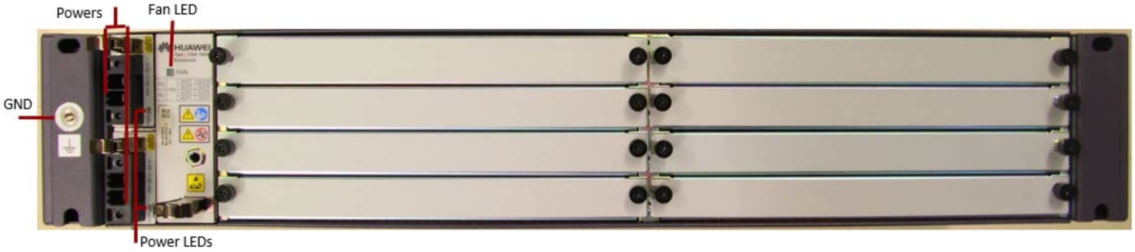


Table 6 - Ports and Interfaces on the Subrack (OSN1800 IIE)

Port	Description	Logical Interface Type
Fan LED	Fan status	Status out
Powers and GND	DC power supply	Power
Power LEDs	Power status	Status out

Figure 5 - Physical Form of the System, Control and Communication Board (TNZ5UXCMS)

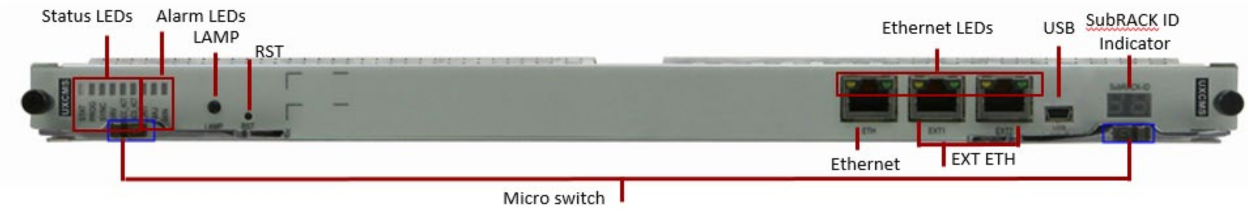


Table 7 - Ports and Interfaces on the System, Control and Communication Board (TNZ5UXCMS)

Port	Description	Logical Interface Type
Ethernet	This is connected to the network port of the network management system (NMS) computer through a network cable so that the NMS can manage the device.	Control in, Data in, Data out, Status out
Status LEDs	Board status (STAT), Program (PROG), Active/standby synchronization status (SYNC), Service (SRV), System control and communication activation (SCC-ACT), Cross-connect and clock activation (XCS-ACT)	Status out
Alarm LEDs	Critical (CTR), Major (MAJ), Minor (MIN)	Status out
Ethernet LEDs	Link status (3), Data status (3)	Status out
Subrack ID Indicator	Indicates the subrack ID.	Status out
RST	Reset button	Control in
Lamp	Not used	N/A
USB	USB interface	Covered with a tamper-evident seal in Approved mode - not accessible
EXT ETH	Port for connecting the master and slave subracks	Covered with a tamper-evident seal in Approved mode - not accessible
Micro switch	The Micro switch is a physical switch used to control removal of a board. It does not correspond with a port or interface.	N/A

Figure 6 - Physical Form of the System, Control and Communication Board (TNZ2UXCL)

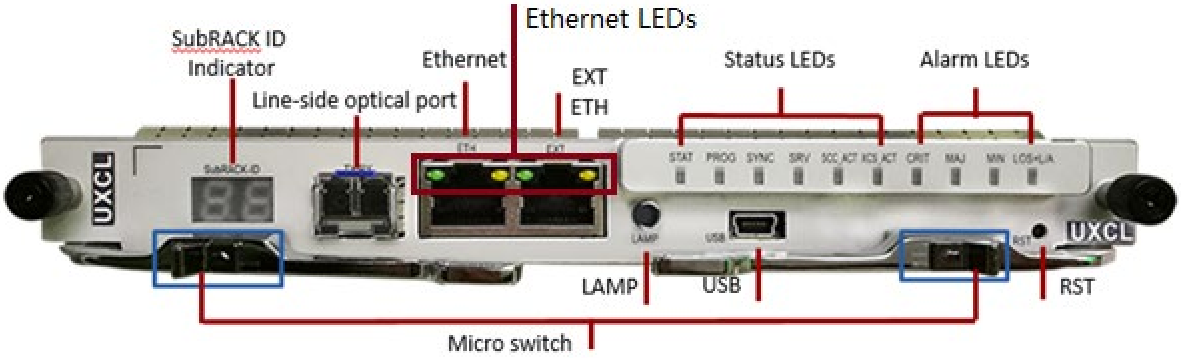


Table 8 - Ports and Interfaces on the System, Control and Communication Board (TNZ2UXCL)

Port	Description	Logical Interface Type
Ethernet	This is connected to the network port of the NMS computer through a network cable so that the NMS can manage the device.	Control in, Data in, Data out, Status out
Status LEDs	Board status (STAT), Program (PROG), Active/standby synchronization status (SYNC), Service (SRV), System control and communication activation (SCC-ACT), Cross-connect and clock activation (XCS-ACT)	Status out
Alarm LEDs	Critical (CTR), Major (MAJ), Minor (MIN), Line-side optical port status (LOS+L/A)	Status out
Ethernet LEDs	Link status (3), Data status (3)	Status out
Subrack ID Indicator	Indicates the subrack ID.	Status out
RST	Reset button	Control in
Lamp	Not used	N/A
Line-side optical port	Transmits / Receives service signals	Data in, Data out
USB	USB interface	Covered with a tamper-evident seal in Approved mode - not accessible
EXT ETH	Port for connecting the master and slave subracks	Covered with a tamper-evident seal in Approved mode - not accessible
Micro switch	The Micro switch is a physical switch used to control removal of a board. It does not correspond with a port or interface.	N/A

Figure 7 - Physical Form of the TNF1CE6

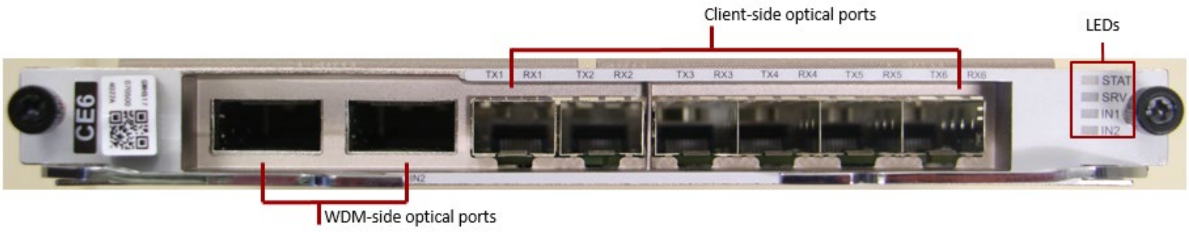


Table 9 - Ports and Interfaces on the TNF1CE6

Port	Description	Logical Interface Type
WDM-side optical ports	Receives / Transmits signals from the optical add / drop multiplexing board of the WDM equipment.	Data in, Data out
Client-side optical ports	Transmits / Receives service signals from client-side equipment.	Data in, Data out
LEDs	Board status (STAT), Service (SRV), WDM-side optical port status (INn (2))	Status out

Figure 8 - Physical Form of the TNF1LDCA

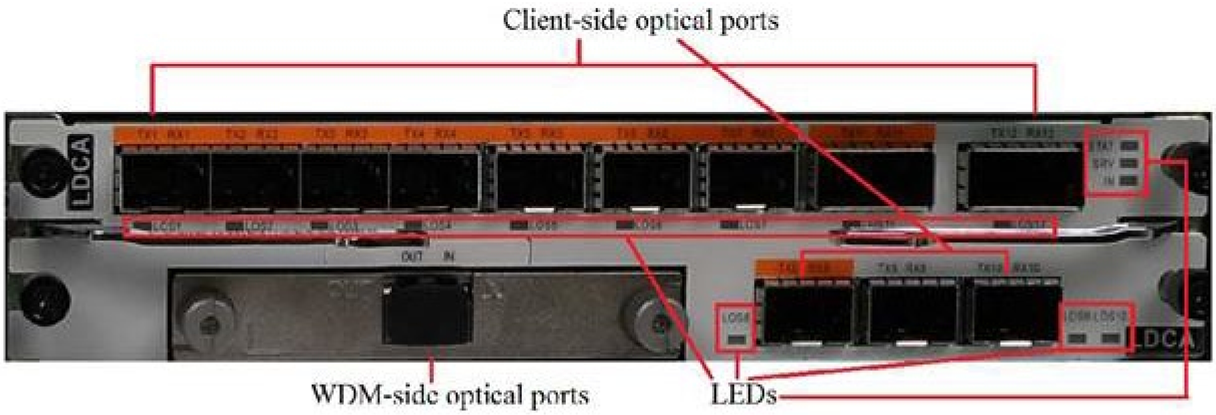


Table 10 - Ports and Interfaces on the TNF1LDCA

Port	Description	Logical Interface Type
WDM-side optical ports	Receives / Transmits signals from the optical add / drop multiplexing board of the WDM equipment.	Data in, Data out
Client-side optical ports	Transmits / Receives service signals from client-side equipment.	Data in, Data out

Port	Description	Logical Interface Type
LEDs	Board status (STAT), Service (SRV), WDM-side optical port status (IN), Client-side optical port status (LOSn (12))	Status out

Figure 9 - Physical Form of the TNF6TTA

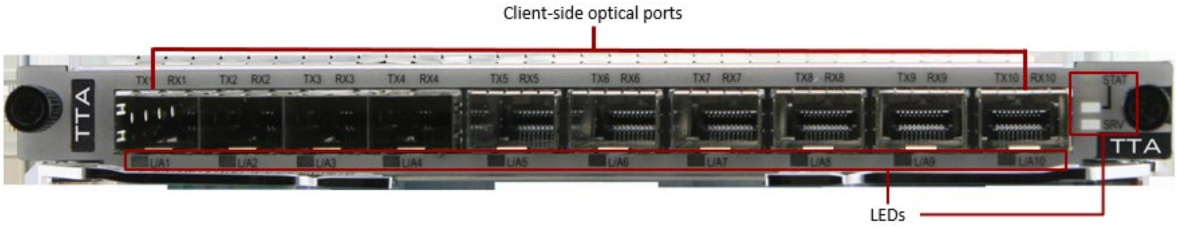


Table 11 - Ports and Interfaces on the TNF6TTA

Port	Description	Logical Interface Type
Client-side optical ports	Transmits / Receives service signals from client-side equipment (Optical port).	Data in, Data out
LEDs	Board status (STAT), Service (SRV), Client-side port status (LOSn (10))	Status out

Figure 10 - Physical Form of the TNZ5UNS4

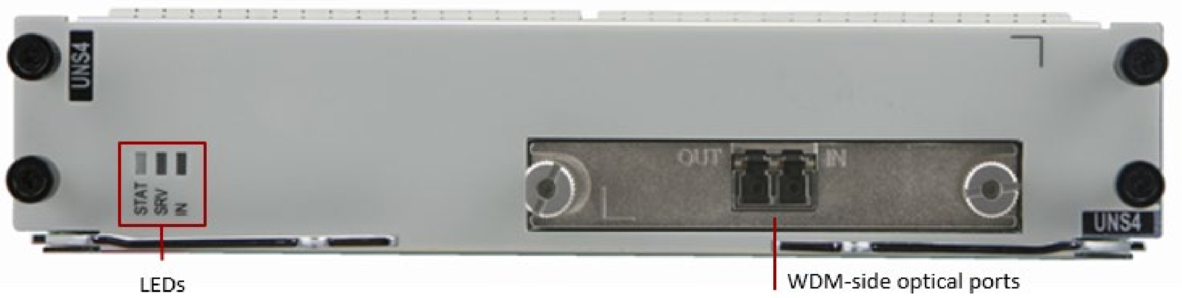


Table 12 - Ports and Interfaces on the TNZ5UNS4

Port	Description	Logical Interface Type
WDM-side optical ports	Receives / Transmits signals from the optical add / drop multiplexing board of the WDM equipment.	Data in, Data out
LEDs	Board status (STAT), Service (SRV), WDM -side port status (IN)	Status out

Figure 11 - Physical Form of the TNF6APIU

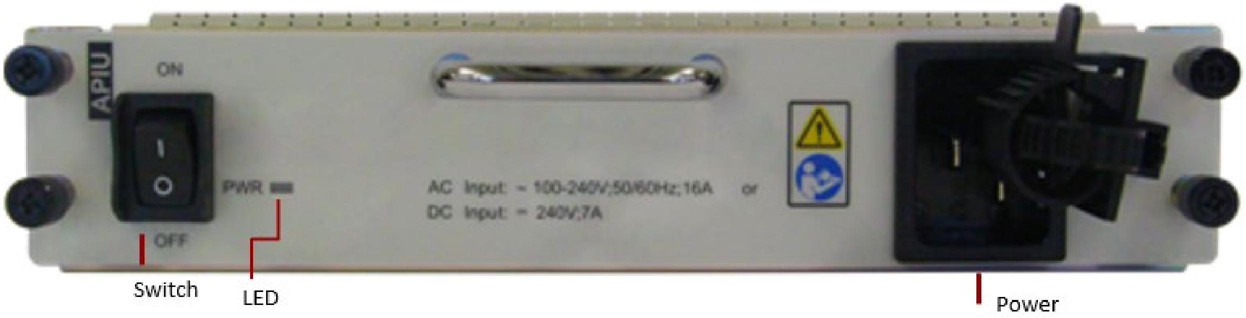


Table 13 - Ports and Interfaces on the TNF6APIU

Port	Description	Logical Interface Type
Switch	Power switch	Control in
LED	Power (PWR) Status (1)	Status out
Power	AC power supply	Power

Figure 12 - Physical Form of the TNZ1APIU

Note: Two (2) separate TNZ1APIU power supplies are placed side-by-side in the picture below.

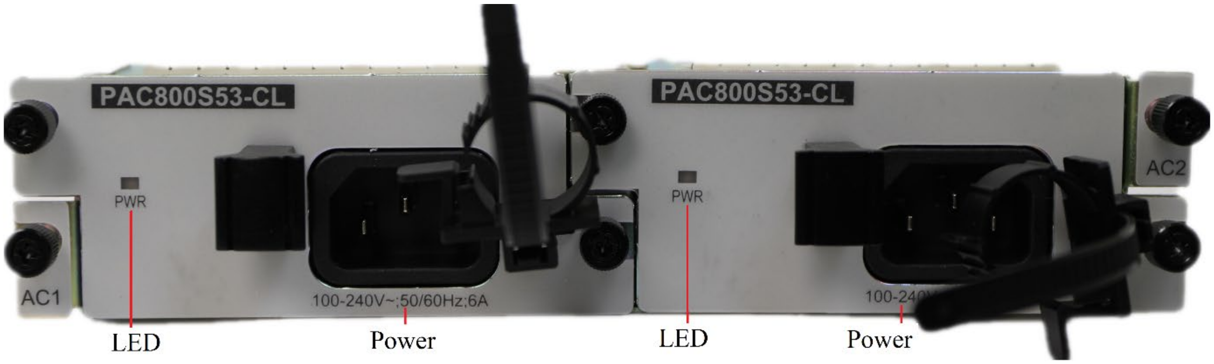


Table 14 - Ports and Interfaces on the TNZ1APIU

Port	Description	Logical Interface Type
LED	PWR Status (1)	Status out
Power	AC power supply	Power

Figure 13 - Physical Form of the TNF5PIU

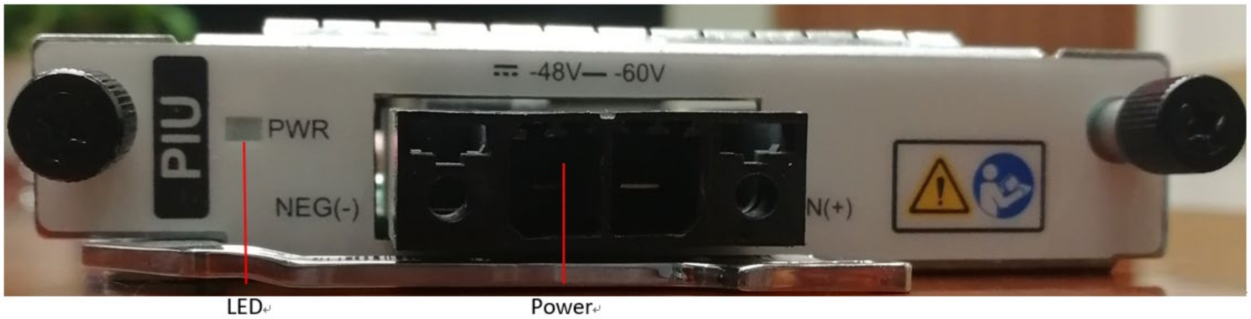


Table 15 - Ports and Interfaces on the TNF5PIU

Port	Description	Logical Interface Type
LED	PWR Status (1)	Status out
Power	DC power supply	Power

Figure 14 - Physical Form of the ANK1PIU

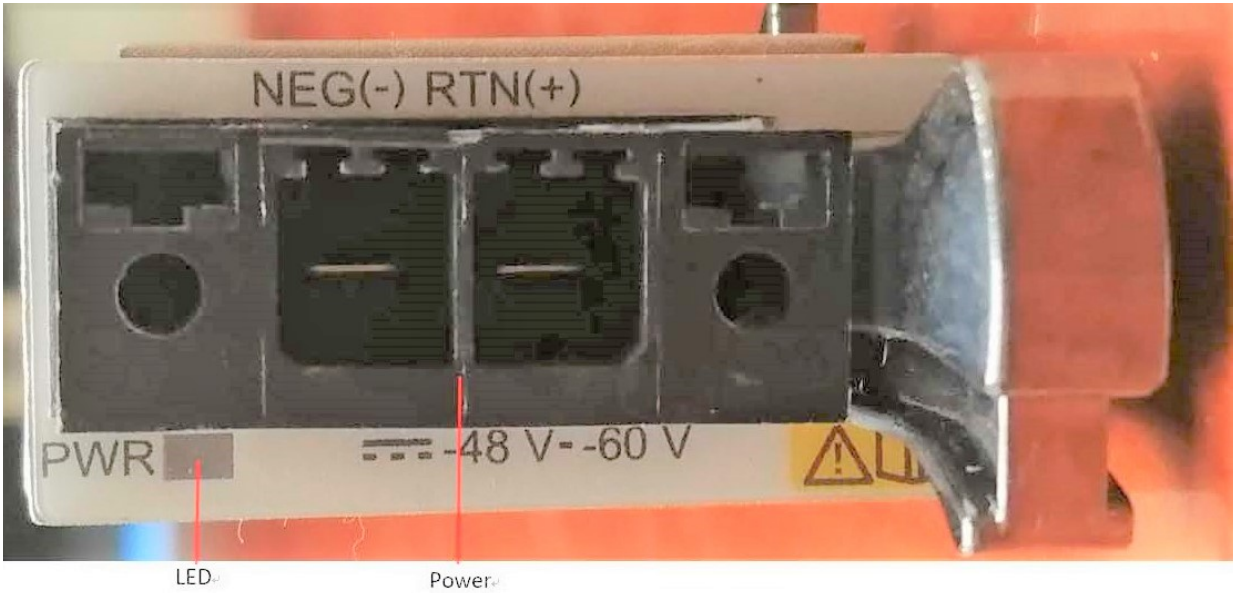


Table 16 - Ports and Interfaces on the ANK1PIU

Port	Description	Logical Interface Type
LED	PWR Status (1)	Status out
Power	DC power supply	Power

1.2 Modes of Operation

The module supports both FIPS and non-FIPS modes of operation. By default, the module comes configured in the non-Approved mode. To verify that a module is in the Approved mode of operation, the user can query the mode by command with an account which is equal or beyond the administrator level. The command is “:fips-get-switch”. If the result shows “enable”, it means the module is in the Approved mode. Run the command “:fips-set-switch:enable/disable” to switch the mode between Approved mode and Non-Approved mode.

The CSPs are not shared between the Approved and non-Approved modes of operation because the CSPs are zeroized when switching from one mode to another.

2. Cryptographic Functionality

The Module implements the FIPS Approved and Non-Approved but Allowed cryptographic functions listed in the tables below.

Table 17 – Approved Algorithms

Cert	Algorithm	Mode	Description	Functions/Caveats
C532	AES [197]	CBC [38A]	Key Sizes: 256	Encrypt, Decrypt
		CTR [38A]	Key Sizes: 256	Encrypt
Vendor Affirmed	CKG [IG D.12]	[133] Section 6.1 Asymmetric signature key generation using unmodified DRBG output		Key Generation[1]
		[133] Section 7.3 Derivation of symmetric keys from a key agreement shared secret.		
C532	CVL: SSH[2] [135]	v2	AES-256 with SHA-1	Key Derivation
	CVL: TLS[3] [135]	v1.1	SHA-1	
		v1.2	SHA (1, 256)	
C532	DRBG [90A]	HMAC	SHA-256	Deterministic Random Bit Generation Security Strength = 256 bits
C532	HMAC [198]	SHA-1	Key Sizes: min 112 bits, Key sizes < block size, Key sizes > block size, Key size = block size λ = 160	Message Authentication

[1] The module directly uses an output U from the Approved HMAC_DRBG.

[2] No parts of these protocols, other than the KDFs, have been tested by the CAVP and CMVP.

[3] No parts of these protocols, other than the KDFs, have been tested by the CAVP and CMVP.

Cert	Algorithm	Mode	Description	Functions/Caveats
		SHA-256	Key Sizes: min 112 bits, Key sizes < block size, Key sizes > block size, Key size = block size λ = 256	
C532	KTS [38F]	AES-CBC AES-CTR	KTS (AES and HMAC)	Key establishment methodology provides 256 bits of encryption strength. HMAC-SHA1 / HMAC-SHA256 is used for the authentication algorithm.
C532	RSA [186]	Key Generation per FIPS 186-4	Key Generation Mode: B.3.3 Modulo: 2048/3072 Primality Tests: C.3	KeyGen

		PKCS1_v1.5	n = 2048 SHA (256)
			n = 3072 SHA (256)
				SigGen

		PKCS1_v1.5	n = 2048 SHA (1, 256)
			n = 3072 SHA (1, 256)
				SigVer

C532	SHS [180]	SHA-1 SHA-256		Message Digest Generation, Password Obfuscation

Table 18 - Non-Approved but Allowed Cryptographic Functions

Algorithm	Description
Diffie-Hellman	This DH version is a variant on PKCS#3 and not the X9.42 specification. No claim is made for NIST SP800-56A. This key agreement scheme is considered Non-Approved but allowed as per IG D.8 Scenario 4 and IG D.11 implementation 2. DH key size: 2048-4096. Diffie-Hellman (CVL Cert. #C532, key agreement; key establishment methodology provides between 112 and 150 bits of encryption strength)
MD5 within TLS	[IG D.2]

Algorithm	Description
NDRNG	Non-Deterministic RNG output is used to seed the FIPS Approved SHA-256 HMAC_DRBG. During seeding, a total of 6144 bits of data from the entropy source are used, and during reseeding, a total of 2048 bits of data from the entropy source are used. The 1800IIE provides at least 0.1552×6144>953 bits of min entropy for seeding and at least 0.1552×2048>317 bits of min entropy for reseeding, which is above the minimum 256 bits of required min entropy. The 1800V provides at least 0.2080×6144>1277 bits of min entropy for seeding and at least 0.2080×2048>425 bits of min entropy for reseeding, which is above the minimum 256 bits of required min entropy. The SHA-256 HMAC_DRBG on all tested devices are able to support a security strength of up to 256 bits.
RSA Key Transport	Supports key length of 2048-3072 bits. It is considered Non-Approved but allowed as per IG D.9 allowed methods for key transport. Moduli for RSA SigGen and SigVer: 2048/3072 bits. Moduli for RSA key transport/wrapping: 2048/3072 bits. Key establishment methodology provides 112 or 128 bits of encryption strength.

Table 19 - Security Relevant Protocols Used in FIPS Mode

Protocol	Key Exchange	Server/ Host Auth	Cipher	Integrity
SSHv2 [IG D.8 and SP 800-135]	Diffie-Hellman-group-exchange-sha1 (2048/3072/4096 bits)	rsa-sha2-256	AES-CTR-256	HMAC-SHA1 HMAC-SHA256
TLS [IG D.8 and SP 800-135]	TLS_RSA_WITH_AES_256_CBC_SHA256			v1.1, v1.2
	RSA	RSA	AES-CBC-256	HMAC-SHA256
	TLS_RSA_WITH_AES_256_CBC_SHA			v1.1, v1.2
	RSA	RSA	AES-CBC-256	HMAC-SHA1
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256			v1.1, v1.2
	DH	RSA	AES-CBC-256	HMAC-SHA2-256
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA			v1.1, v1.2
	DH	RSA	AES-CBC-256	HMAC-SHA1
OSPF/RSVP	NA	NA	NA	HMAC-SHA256

Non-Approved Cryptographic Functions for use in non-FIPS mode only:

- DES
- MD5
- HMAC-SHA1-96
- HMAC-MD5
- HMAC-MD5-96

Approved Cryptographic Functions implemented by Huawei FIPS Cryptographic Library (HFCL), but not used / reachable:

- Hash/CTR-DRBG
- DSA Key Gen, Sig Gen, Sig Ver
- ECC CDH
- ECDSA Key Pair Gen, Sig Gen, Sig Ver
- AES/TDES-CMAC
- AES-GCM/GMAC
- TDES

2.1 Critical Security Parameters

All CSPs used by the Module are described in this section. All usage of these CSPs by the Module (including all CSP lifecycle states) is described in the services detailed in Section 4.

Table 20 - Critical Security Parameters (CSPs)

CSP	Description / Usage
DRBG-EI	DRBG entropy input. During seeding, a total of 6144 bits of entropy data are gathered directly from the entropy source. During reseeding, a total of 2048 bits of entropy data are gathered directly from the entropy source.
DRBG-State	HMAC_DRBG internal state (V and Key)
AUTH-PW	Authentication Passwords, minimum of 8 characters.
SSH-DH-Priv	(SSHv2 Diffie-Hellman ephemeral) modules=2048/3072/4096
SSH-Host-Priv	(SSHv2 Host Key) RSA n=2048/3072 Private Key
SSH-SENC	(SSHv2 Session Encryption Key) AES CTR 256 keys
SSH-SMAC	(SSHv2 Session Authentication Keys) HMAC-SHA1 160-bit key and HMAC-SHA256 256-bit key
TLS-DH-Priv	(TLS Diffie-Hellman) L=2048/3072/4096 Private Key
TLS-Host-Priv	(TLS Host Key) RSA n=2048/3072 Private Key

CSP	Description / Usage
TLS-MS	(TLS Master Secret) 384-bit secret key material
TLS-PMS	(TLS Pre-Master Secret) 384-bit secret key material
TLS-SENC	(TLS Session Encryption Key) AES CBC 256-bit key
TLS-SMAC	(TLS Session Authentication Keys) HMAC-SHA1 (160-bit key) or HMAC-SHA256 (256-bit key)
External Pre-Shared Key	HMAC-SHA256 pre-shared key of authentication for OSPF/RSVP protocols. The External Pre-Shared Key is configured by the operator. OSPF/RSVP protocols use this key to calculate the HMAC-SHA256 value with protocol packets and send the value to the peer. If the value that was sent is equal to the value recalculated by the peer using the configured key upon receiving the packet, then the packet is accepted. Otherwise, it is dropped.

2.2 Public Keys

Table 21 – Public Keys

Key	Description / Usage
SSH-Host-Pub	(SSHv2 Host Key) RSA 2048/3072 public key
SSH-DH-Pub	SSHv2 Diffie-Hellman 2048/3072/4096 server public key
SSH-RSA-CLI-Pub	SSHv2 RSA 2048/3072 client public key
TLS-Host-Pub	(TLS Host Key) RSA 2048/3072 public key
TLS-DH-Pub	TLS Diffie-Hellman 2048/3072/4096 public Key
FW-Pub	Firmware Publication Public Key

3. Roles, Authentication and Services

3.1 Assumption of Roles

The module supports five (5) distinct operator levels, super administrator, administrator, maintenance, operation account, and monitor. Super administrator, administrator and maintenance account are mapped to Crypto Officer Role. Operation account and monitor account are mapped to User Role. Re-authentication is enforced when changing account and rebooting. The maintenance operator level is given that name in the context of the product. This is not the same thing as the Maintenance role as defined in FIPS 140-2. There is neither a FIPS 140-2 Maintenance interface nor Maintenance mode.

Table 22 lists all operator roles supported by the Module. The Module does not support a maintenance role and bypass capability. The Module supports concurrent operators. Users using different accounts can log in to device from different terminals at the same time. Login users are independent of each other. Authentication status does not persist across power cycles. After rebooting, users need re-authentication with correct username and password. The password hash (SHA256) value is stored in database in flash. All users shall authenticate successfully before they can execute command. The users' password input will be masked by stars.

Table 22 – Roles Description

Role ID	Role Description	Authentication Type	Authentication Data
Monitor	User Role. Used for info query.	Identity-based (using *Local password verification or public key*)	Username and password or public key
Operation	User Role. Used for basic configuration.		
Maintenance	Crypto Officer Role. Run commands belong to maintenance level		
Administrator	Crypto Officer Role. Manage accounts and run other commands belong to administrator level		
Super administrator	Crypto Officer Role. A special type of administrator and can be used to run debug commands.		

3.2 Authentication Methods

Table 23 – Authentication Description

Authentication Method	Probability	Justification
Username and password authentication	The odds of guessing a password is 1/ (94^8), which is significantly less than 1/1,000,000. The probability of successfully authenticating to the module within one minute is 10/ (94^8), which is less than 1/100,000.	The minimum password length is eight (8) characters. The password must contain at least three (3) types of the following characters: uppercase letters (A to Z), lowercase letters (a to z), digits (0 to 9), and 32 special characters. The odds of guessing a password is 1/ (94^8), which is significantly less than 1/1,000,000. The module supports lockout mechanism, which disables a user account after a configured number of unsuccessful attempts to authenticate. A locked-out user cannot successfully log in again until the user account is unlocked. The module may be configured with a worst-case scenario of having the authentication limit counter set to 10 times per minute (however, five times is the default). The probability of successfully authenticating to the module within one minute is 10/ (94^8), which is less than 1/100,000. The password entry feedback mechanism does not provide information that could be used to guess or determine the authentication data.

Authentication Method	Probability	Justification
Public key-based authentication	The probability that a random attempt will succeed is 1/(2^112) which is less than 1/1,000,000. The probability of successfully authenticating to the module within a one-minute period is 15/(2^112), which is less than 1/100,000.	The module supports SSH certificate-based authentication using RSA 2048, 3072. The minimum equivalent strength supported by the module is 112 bits. The module is able to perform 15 authentication attempts per minute. Before initiating public key-based authentication, the SSH connection must first be established. DH negotiation is necessary while establishing the SSH connection. The module has a one minute timer. If the DH negotiation has reached 10 times within one minute, then it will be delayed 200ms to handle the next one. Counting the DH calculation time, the module deals a maximum of 15 times DH negotiations in one minute. Therefore, there is a limit of 15 times public key-based authentication can be attempted in one minute.

3.3 Services

All services implemented by the Module are listed in the tables below.

Table 24 – Authenticated Services

Service	Description	CO	U
Zeroization - Initialize Database (Reset to Factory Defaults)	Restoring the module to factory conditions via command is the means of providing zeroization keys and CSPs. The command is ":dbms-delete-data".	X	
Module Reset	Rebooting the module via the reset command. This service executes the suite of self-tests required by FIPS 140-2 and initialize DRBG. The command is ": reset".	X	

Service	Description	CO	U
System Management	Basic configuration and other high-level configuration (fault diagnosis, system configure, CSPs operation, firmware update, RSA keys management, TLS certificates management).	X	X
Status Monitoring and Reporting	The “Show Status” service, including Monitor, providing module status (CPU usage, alarm, performance, etc.) and logs.	X	X
User Management	Create/Delete/Modify users	X	X
SSH protocol	Provide communication security between the Module and management terminal	X	X
TLS protocol	Provide communication security between the Module and management terminal	X	X
Zeroization - Mode switch	Switch to Approved or non-Approved mode. When switched to Approved mode, it will execute the suite of self-tests required by FIPS 140-2 and initialize DRBG. The command “:fips-set-switch:enable/disable” is used to switch the mode of operation.	X	

The services listed in Table 24 are also available in the non-FIPS mode of operation and can be used with non-Approved security functions listed at the end of section 2.

Table 25 – Unauthenticated Services

Service	Description
Module Reset via the reset button (Includes Self-test)	Rebooting the module via the reset button. This service executes the suite of self-tests required by FIPS 140-2 and initialize DRBG.

Table 26 – Services Only Available in Non-FIPS Mode

Service	Description
FTP	FTP protocol
SNMP	SNMP protocol
Telnet	Telnet protocol
SFTP	SFTP protocol
RADIUS	RADIUS protocol

Table 27 defines the relationship between access to Security Parameters and the different module services. The modes of access shown in the table are defined as:

- G = Generate: The service generates the CSP.
- O = Output: The service outputs the CSP.
- E = Execute: The service uses the CSP in an algorithm.
- I = Input: The service inputs the CSP.
- Z = Zeroize: The service zeroizes the CSP.

Table 27 - Security Parameters Access by Service

Service	CSPs and Public Keys																			
	DRBG EI	DRBG-State	AUTH-PW	SSH-DH-Priv	SSH-Host-Priv	SSH-SENC	SSH-SMAC	TLS-DH-Priv	TLS-Host-Priv	TLS-MS	TLS-PMS	TLS-SENC	TLS-SMAC	External Pre-Shared Key	SSH-Host-Pub	SSH-DH -Pub	SSH-RSA-CLI-Pub	TLS-Host-Pub	TLS-DH-Pub	FW-Pub
Zeroization - Initialize Database (Reset to Factory Defaults)	-	-	EZ	-	-	-	-	-	-	-	-	-	-	Z	-	-	EZ	-	-	-
Module Reset	GEZ	GZ	E	Z	-	Z	Z	Z	-	Z	Z	Z	Z	-	-	Z	E	-	Z	-
System Management	-	-	E	-	GZ	E	E	-	EIZ	-	-	E	E	EIZ	GZ	-	EI	EIZ	-	E
Status Monitoring and Reporting	-	-	E	-	-	-	-	-	-	-	-	-	-	-	-	-	E	-	-	-
User Management	-	E	EIZ	-	-	-	-	-	-	-	-	-	-	-	-	-	E	-	-	-
SSH protocol	-	E	-	GEZ	E	GEZ	GEZ	-	-	-	-	-	-	-	E	GEZ		-	-	-
TLS protocol	-	E	-	-	-	-	-	GEZ	E	GEZ	GEZ	GEZ	GEZ	-	-	-	-	E	GEOZ	-
Zeroization - Mode switch	GEZ	GZ	EZ	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	EZ	Z	Z	-
Module Reset via the reset button (Includes Self-test)	GEZ	GZ	-	Z	-	Z	Z	Z	-	Z	Z	Z	Z	-	-	Z	-	-	Z	-

4. Self-Tests

The module performs self-tests to ensure the proper operation of the module. Per FIPS 140-2 these are categorized as either power-up self-tests or conditional self-tests. Power up self–tests are available on demand via the reset button, by power cycling the module, or running the reboot command ": reset".

All algorithm Known Answer Tests (KATs) must be completed successfully prior to any other use of cryptography by the Module. If one of the KATs fails, the Module enters the error state and outputs status by a red LED flashing for five (5) seconds, otherwise it indicates successful completion by a green LED light.

Table 28 - Algorithm KATs on Power-up

Test Target (Cert. #)	Description
Firmware Integrity	32-bit CRC for boot loader Integrity check and SHA-256 for firmware Integrity check.
AES (Cert. #C532)	Separate encrypt, decrypt KATs using 256-bit keys and CBC/CTR.
DRBG (Cert. #C532)	HMAC-SHA256 DRBG KAT. Performed conditionally (where initial use at power-up is the condition) per SP 800-90 Section 11.3.
HMAC (Cert. #C532)	Separate HMAC generation and verification KATs.
RSA (Cert. #C532)	Separate KATs of signature generation and signature verification for n=2048 and 3072 bits.
SHS (Cert. #C532)	KAT of SHA-1 SHA-256 is tested as part of the HMAC-SHA-256 KATs as per IG 9.2.

Table 29 – Conditional Tests

Test Target	Description
RNG	Continuous RNG Test for the DRBG is performed on each RNG access.
RSA	RSA Pairwise Consistency Test is performed on each RSA key pair generation.
ENTROPY	Repetition Count Test and Adaptive Proportion Test are performed on each entropy get from the NDRNG.
FW load	RSA 2048 and SHA256 are used to test the firmware loading procedure.

Table 30 - Critical Functions Tests

Critical function	API	Description
DRBG initialization	InitDrbg	It is run on the power-up process. Health testing is also performed. If it fails, the module will restart.
Get the flag that indicates whether the module is in FIPS/Non-FIPS mode from flash	FipsGetStoredMode	It is run on the power-up process. SHA256 is used for checking the integrity. If it fails, the module will restart.

5. Physical Security Policy

The cryptographic modules each include the following physical security mechanisms:

- Production-grade components and production-grade opaque enclosure
- Tamper-evident seals applied on the surfaces of the module
- Protected vents

The HUAWEI OptiX OSN 1800 V and OptiX OSN 1800 IIE are multi-chip standalone modules that contain production quality standard passivation. Chip components are protected by an opaque enclosure. There are tamper-evident seals that are applied on the modules by the CO. All unused seals are to be controlled by the CO. The seals prevent removal of the opaque enclosure without evidence.

For application of the tamper-evident seals, the CO must ensure that the module surface is clean and dry. Tamper-evident seals must be pressed firmly onto the adhering surfaces during installation and once applied, the CO shall permit 24 hours of cure time for all tamper-evident seals. The CO should inspect the seals and shields for evidence of tamper every 30 days. If the seals show evidence of tamper, the CO should assume that the modules have been compromised and contact Customer Support.

The following is the installation location of each product tamper-evident seal for two (2) sample configurations – AC and DC power – for each module.

Figure 15 through Figure 18 show the installation locations of HUAWEI OptiX OSN 1800 V (DC Power) tamper-evident seals. A total of 25 seals must be applied as prescribed. The USB port and EXT ports shall be directly covered with seals.

Figure 19 through Figure 21 show the installation locations of HUAWEI OptiX OSN 1800 V (AC Power) tamper-evident seals. A total of 23 seals must be applied as prescribed. The differences between the DC and AC tamper-evident seal placement is that Seal #16 is in a slightly different location on the AC configuration and Seals #18 & #19 in the DC configuration are for blank faceplates. The seals must cover every slot so that all the cards and blank faceplates installed in the chassis cannot be removed without damaging the seals. The USB port and EXT ports shall be directly covered with seals.

Figure 15 – OSN 1800 V (DC Power) Tamper-Evident Seal Locations (Front)

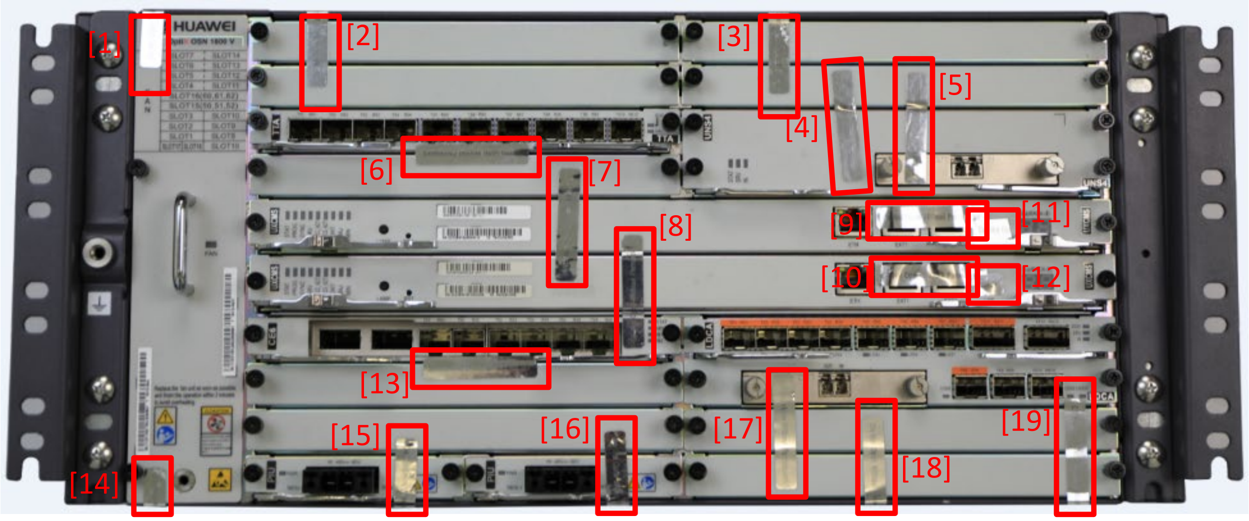


Figure 16 – OSN 1800 V (DC Power) Tamper-Evident Seal Locations (Bottom)

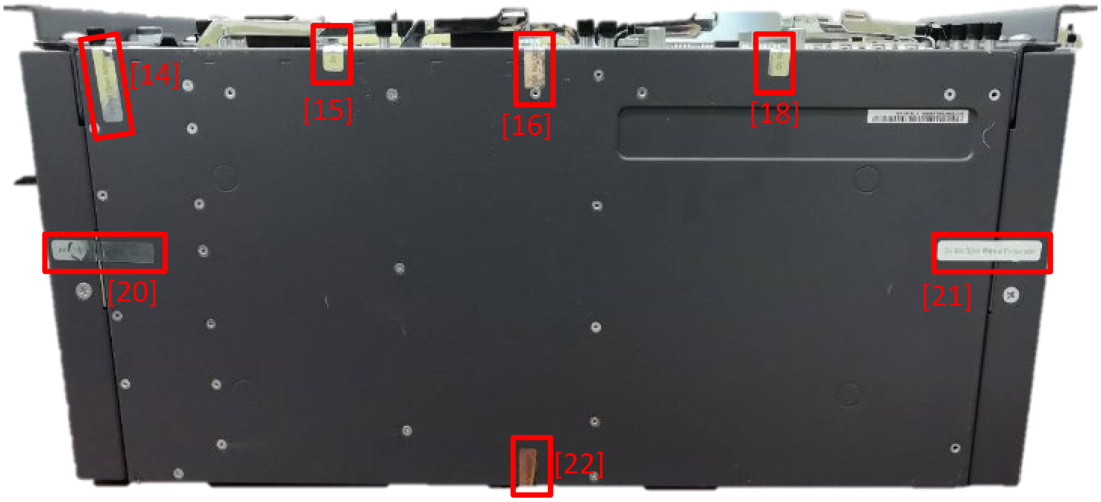


Figure 17 – OSN 1800 V (DC Power) Tamper-Evident Seal Locations (Top)

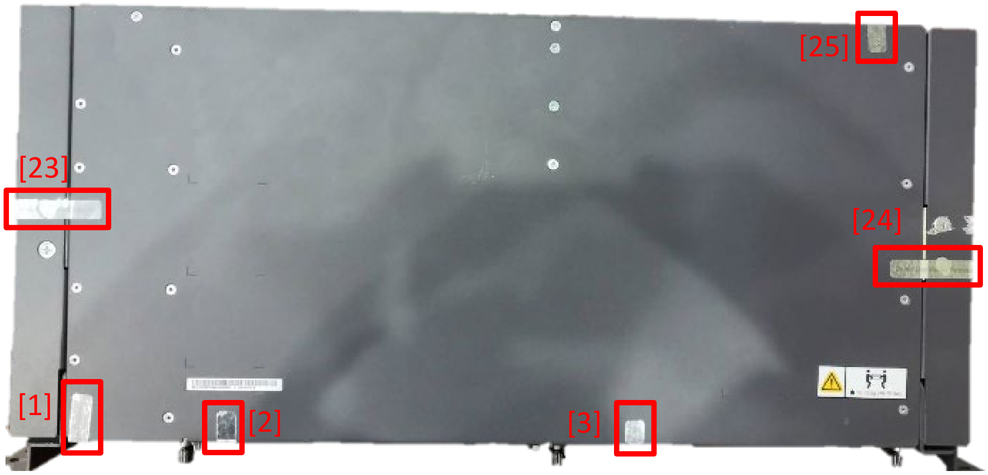


Figure 18 – OSN 1800 V (DC Power) Tamper-Evident Seal Locations (Back)

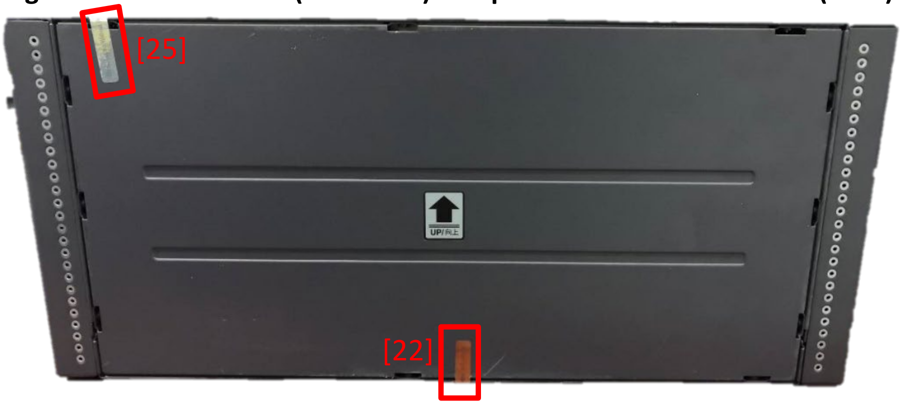


Figure 19 – OSN 1800 V (AC Power) Tamper-Evident Seal Locations (Front)

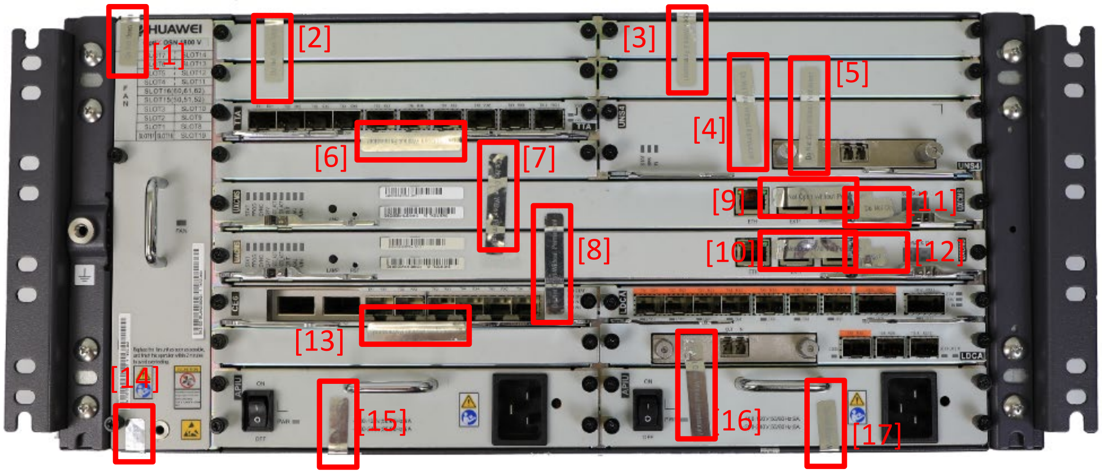


Figure 20 – OSN 1800 V (AC Power) Tamper-Evident Seal Locations (Bottom)

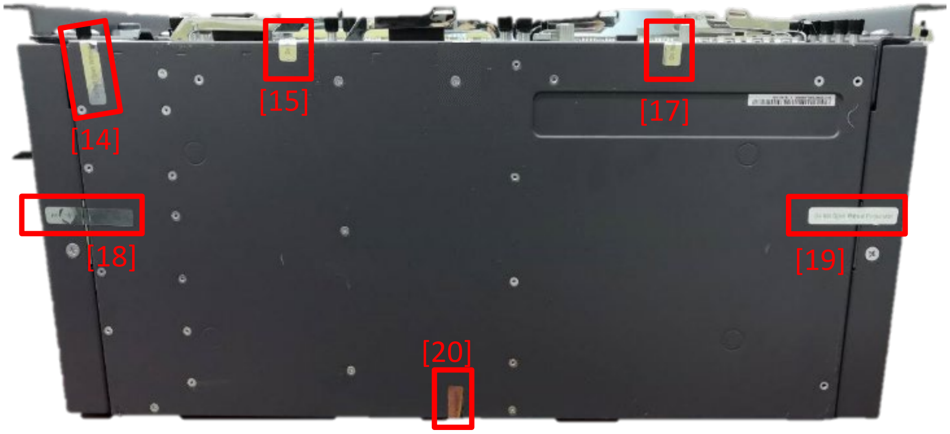


Figure 21 – OSN 1800 V (AC Power) Tamper-Evident Seal Locations (Top)

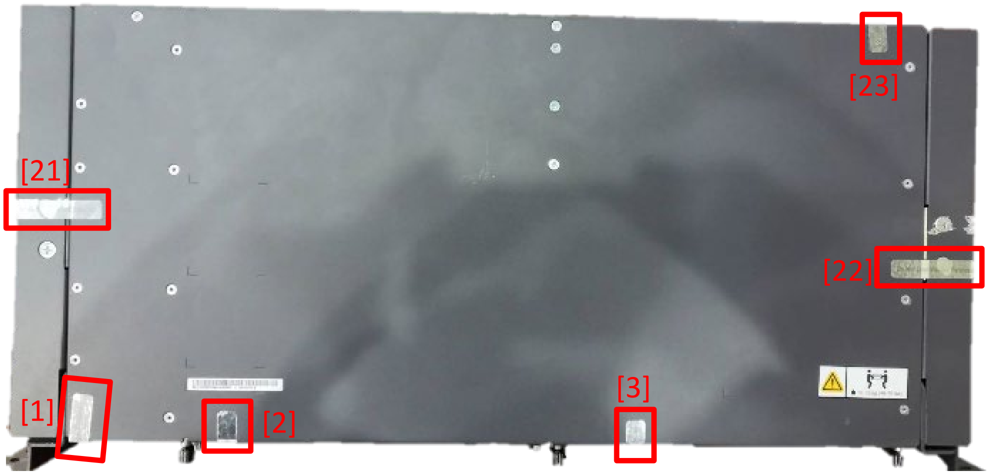


Figure 22 – OSN 1800 V (AC Power) Tamper-Evident Seal Locations (Back)

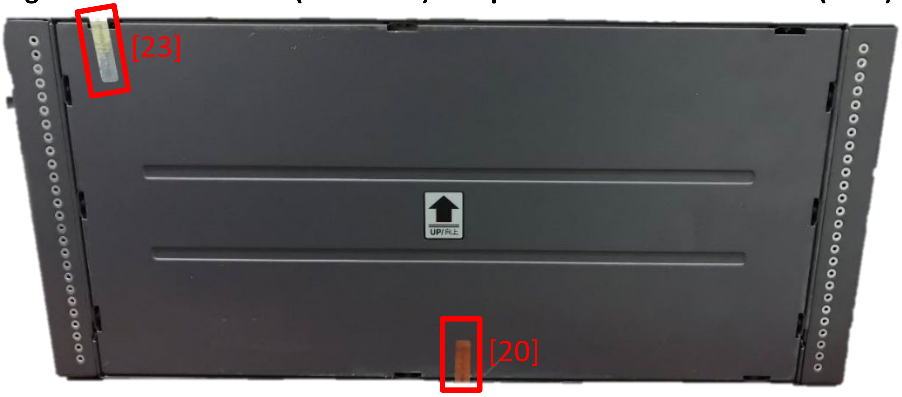


Figure 23 - OSN 1800V (Right Side)

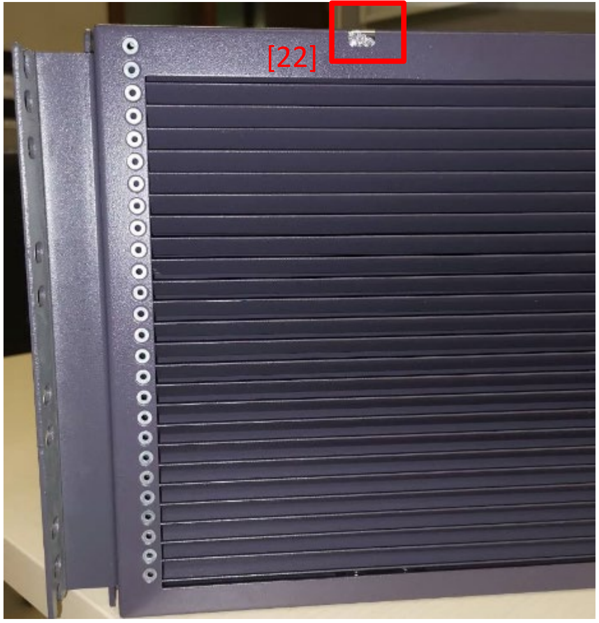


Figure 24 OSN - 1800V (Left Side)

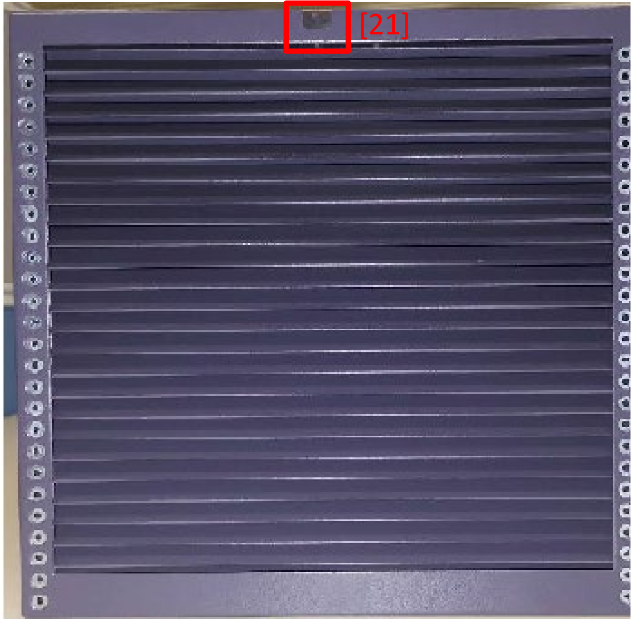


Figure 25 through Figure 28 show the installation locations of HUAWEI OptiX OSN 1800IIE (AC Power) tamper-evident seals. A total of 19 seals must be applied as prescribed. The seals must cover every slot so that all the cards and blank faceplates installed in the chassis cannot be removed without damaging the seals. The USB port and EXT ports shall be directly covered with seals.

Figure 29 through Figure 32 show the installation locations of HUAWEI OptiX OSN 1800IIE (DC Power) tamper-evident seals. A total of 18 seals must be applied as prescribed. The differences between the DC and AC tamper-evident seal placement is that Seal #1 in the AC unit is not required on the DC unit and the DC configuration has slightly difference seal locations on the front (#11 & #12) for blank faceplates. The seals must cover every slot so that all the cards and blank faceplates installed in the chassis cannot be removed without damaging the seals. The USB port and EXT ports shall be directly covered with seals.

> Note: The tamper-evident seals cannot be applied in their correct locations if the cards are not placed in their proper order as shown in Figure 25 through Figure 32.

Figure 25 - OSN 1800IIE (AC Power) Tamper-Evident Seal Locations (Front)

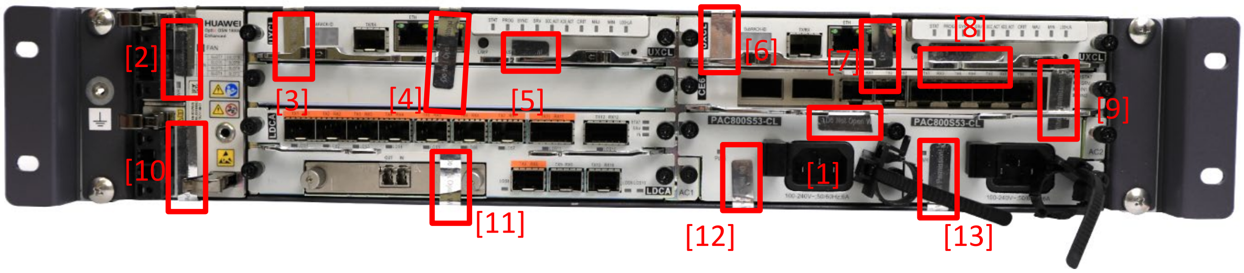


Figure 26 – OSN 1800IIE (AC Power) Tamper-Evident Seal Locations (Top)

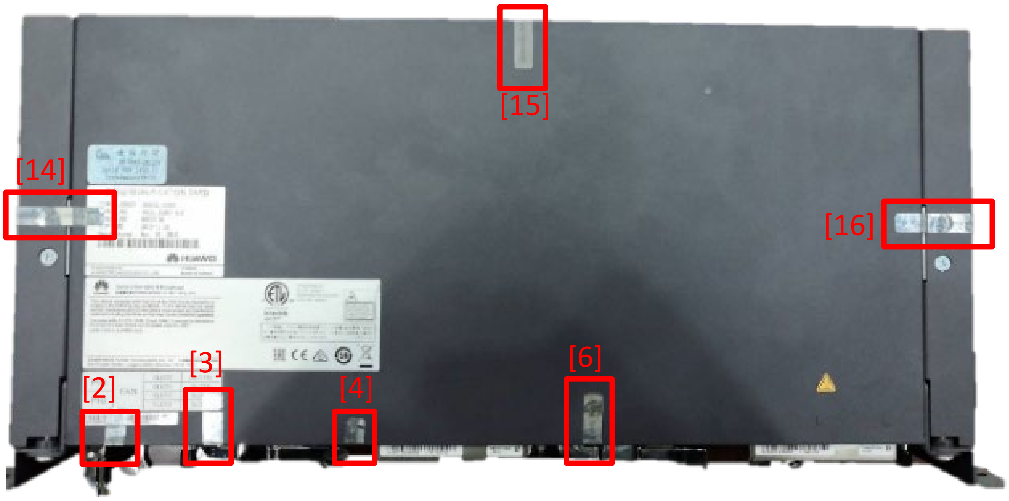


Figure 27 – OSN 1800IIE (AC Power) Tamper-Evident Seal Locations (Bottom)

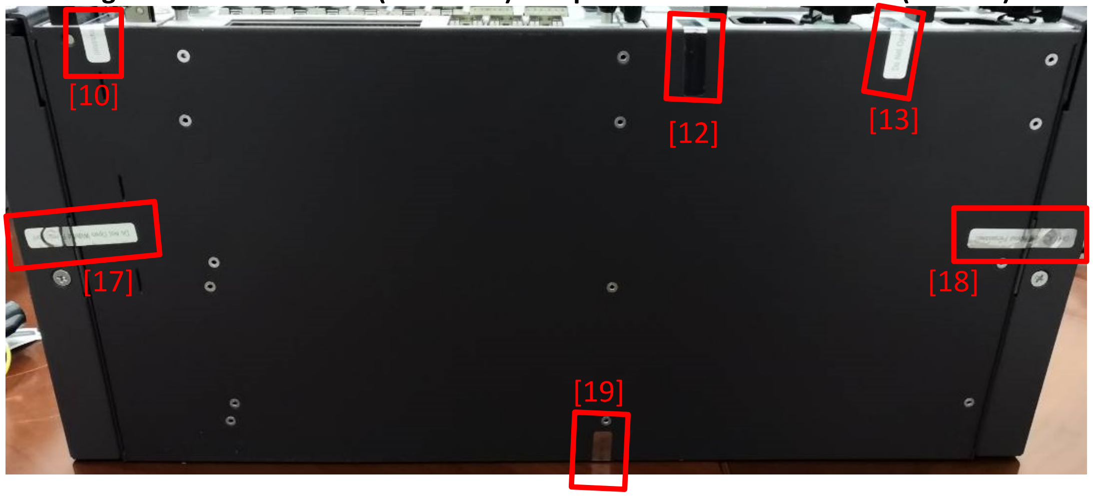


Figure 28 – OSN 1800IIE (AC Power) Tamper-Evident Seal Locations (Back)

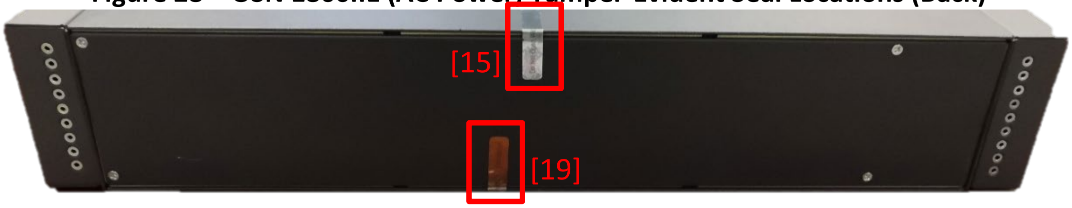


Figure 29 – OSN 1800IIE (DC Power) Tamper-Evident Seal Locations (Front)

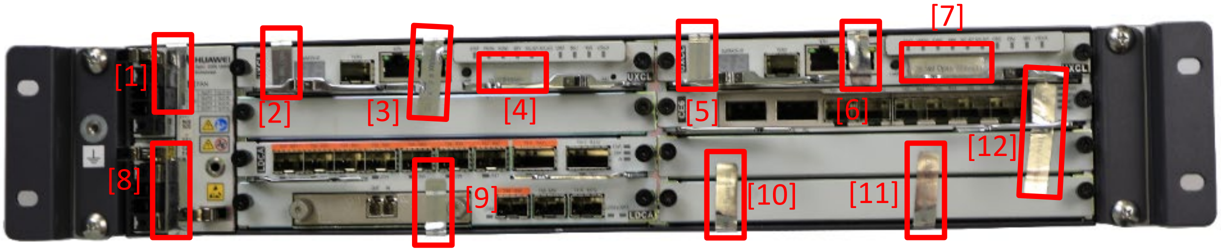


Figure 30 – OSN 1800IIE (DC Power) Tamper-Evident Seal Locations (Top)

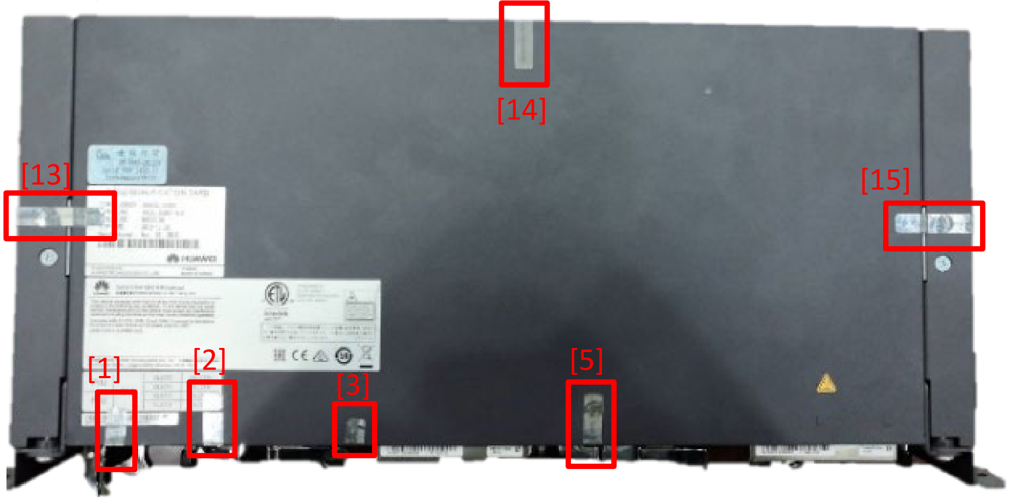


Figure 31 – OSN 1800IIE (DC Power) Tamper-Evident Seal Locations (Bottom)

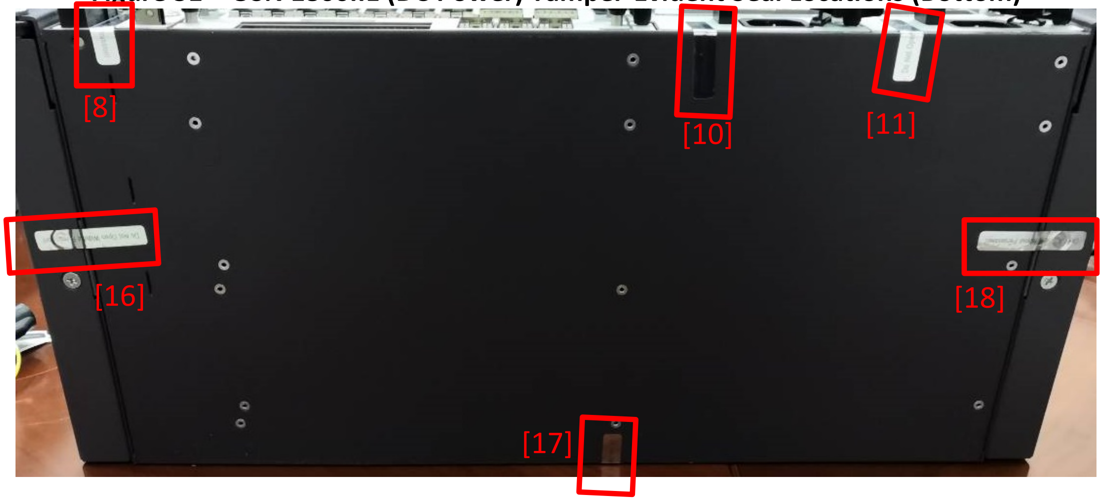
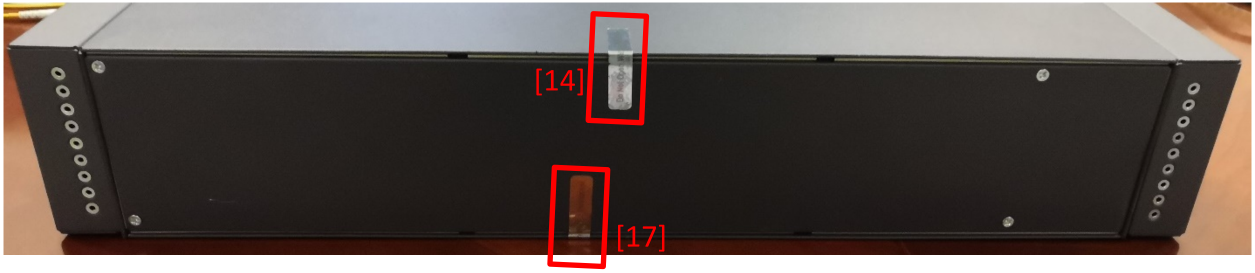


Figure 32 – OSN 1800IIE (DC Power) Tamper-Evident Seal Locations (Back)



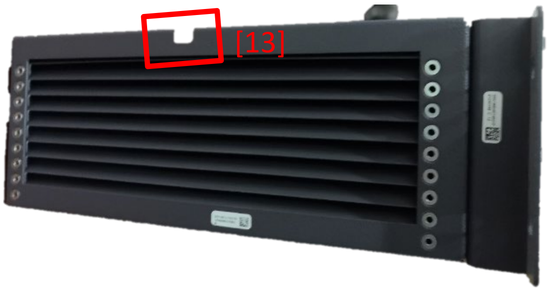


Figure 33: OSN 1800 IIE (Left Side)

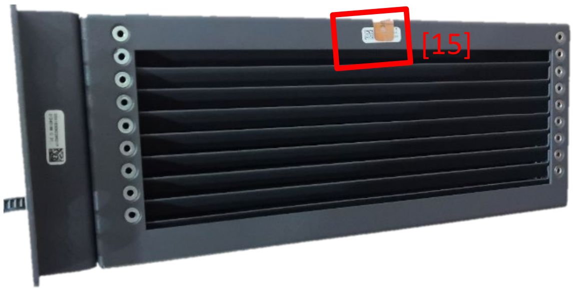


Figure 34: OSN 1800 IIE (Right Side)

Note: The other labels not identified by brackets are manufacturing labels.

6. Operational Environment

The Module has a limited operational environment under the FIPS 140-2 definitions. The Module includes a firmware load service to support necessary updates. Firmware versions validated through the FIPS 140-2 CMVP will be explicitly identified on a validation certificate. Any firmware not identified in this Security Policy does not constitute the Module defined by this Security Policy or covered by this validation.

7. Mitigation of Other Attacks Policy

The module has not been designed to mitigate attacks outside the scope of FIPS 140-2

8. Security Rules and Guidance

This section documents the security rules for the secure operation of the cryptographic module to implement the security requirements of FIPS 140-2.

The module implementation enforces the following security rules:

1. The module supports five (5) distinct operator levels, super administrator, administrator, maintenance, operation account and monitor.
2. The module provides identity-based authentication.
3. The module clears previous authentications on power cycle.
4. An operator does not have access to any cryptographic services prior to assuming an authorized role.
5. The module allows the operator to initiate power-up self-tests by power cycling power or resetting the module.
6. Power up self-tests do not require any operator action.

7. Data output are inhibited during key generation, self-tests, zeroization, and error states.
8. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
9. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
10. The module supports concurrent operators.
11. The module does not support a maintenance interface or role.
12. The module does not support manual key entry.
13. The module does not have any proprietary external input/output devices used for entry/output of data.
14. Manual key output is not supported.
15. The module does not output intermediate key values.
16. The module is seeded with 6144 bits of entropy data and reseeded where applicable, with 2048 bits of entropy data.
17. The module does not provide bypass services or ports/interfaces.
18. The DH key is at least 2048 bits and gets the random from the approved DRBG output. And only AES-256 is used in KTS and provides 256 bits of encryption strength. So, compromising the security of the algorithm used for key establishment will require as many operations as determining the value of the cryptographic key being transported or agreed upon.

The user shall enforce the following security rules:

19. The operator must not configure the authentication limit counter to more than 10.
20. The operator must apply the tamper seals as indicated above in Section 5 Physical Security Policy.
21. Run the command ":fips-set-switch:enable/disable" to switch the mode between Approved mode and Non-Approved mode. The command ":fips-set-switch:enable" is used to switch the module to Approved mode and no more operation is needed.

The secure installation, initialization, and start-up procedures are:

Installation:

1. Check tamper-evident seals as per Section 5 Physical Security.
2. Do hardware installation.
3. Connect power supply to the module.

Initialization:

1. Power up the module.
2. Login as a CO with the default password, e.g. an Administrator or Super Administrator account.
3. Change the password as prompted.

4. Check the version using the command “display version”. The version shall match the one identified in Table 1 of the Security Policy:
    a. OSN1800 V: V100R009C00SPC300 5.67.09.16T26
    b. OSN1800 IIE: V100R009C00SPC300 5.67.09.16T26
5. Run the command “fips-set-switch:enable” to switch to FIPS mode.
6. Note: the module reboots immediately to switch to FIPS mode.

Start-up:

1. Power up the module.
2. Login as a CO.
3. Run the command “fips-get-switch”. If the result shows “enable”, it means the module is operating in FIPS mode.

9. References and Definitions

The following standards are referred to in this Security Policy.

Table 31 - References

Abbreviation	Full Specification Name
[FIPS140-2]	*Security Requirements for Cryptographic Modules*, May 25, 2001
[IG]	*Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program*
[108]	*NIST Special Publication 800-108, Recommendation for Key Derivation Using Pseudorandom Functions (Revised), October 2009*
[131Ar2]	*NIST Special Publication 800-131A Rev. 2, Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, March 2019*
[132]	*NIST Special Publication 800-132, Recommendation for Password-Based Key Derivation, Part 1: Storage Applications, December 2010*
[133r1]	*NIST Special Publication 800-133 Rev. 1, Recommendation for Cryptographic Key Generation, July 2019*
[135]	*National Institute of Standards and Technology, Recommendation for Existing Application-Specific Key Derivation Functions, Special Publication 800-135rev1, December 2011.*
[186-4]	*National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-4, July, 2013.*
[186-2]	*National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-2, January 2000.*
[197]	*National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001*
[198]	*National Institute of Standards and Technology, The Keyed-Hash Message Authentication Code (HMAC), Federal Information Processing Standards Publication 198-1, July, 2008*
[180]	*National Institute of Standards and Technology, Secure Hash Standard, Federal Information Processing Standards Publication 180-4, August, 2015*
[202]	*FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, FIPS PUB 202, August 2015*
[38A]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, December 2001*

Abbreviation	Full Specification Name
[38B]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Special Publication 800-38B, October 2016*
[38C]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, Special Publication 800-38C, August 2007*
[38D]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, Special Publication 800-38D, November 2007*
[38F]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, Special Publication 800-38F, December 2012*
[56A]	*NIST Special Publication 800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised), March 2007*
[56Ar3]	*NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, April 2018*
[56Br2]	*NIST Special Publication 800-56A Revision 2, Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography, March 2019*
[67r2]	*National Institute of Standards and Technology, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Special Publication 800-67 Revision 2, November 2017*
[90Ar1]	*National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A Revision 1, June 2015.*
[90B]	*National Institute of Standards and Technology, Recommendation for the Entropy Sources Used for Random Bit Generation, Special Publication 800-90B, January 2018.*
SSH	*Ylonen, T. and C. Lonvick, "The Secure Shell (SSH) Connection Protocol", RFC 4252/4253/4254, Internet Engineering Task Force, January 2006.* *D. Bider, "Use of RSA Keys with SHA-256 and SHA-512 in the Secure Shell (SSH) Protocol", RFC 8332, Internet Engineering Task Force, March 2018.*
TLS	*Dierks, T., and E. Rescoria, "The Transport Layer Security (TLS) Protocol Version 1.2". RFC 5246, Internet Engineering Task Force, August 2008.*

Table 32 - Acronyms and Definitions

Acronym	Definition
IETF	Internet Engineering Task Force, a standards body
NMS	Network Management System
OSPF	Open Shortest Path First; Routing Protocol
RFC	Request For Comment; the prefix used by IETF for internet specifications.
RSVP	Resource Reservation Protocol; a Quality of Service network protocol to reserve resources.
SSH	Secure Shell
TLS	Transport Layer Security
TCP	Transmission Control Protocol
WDM	Wavelength-Division Multiplexing