Infinera Corporation
Infinera Groove G30 DCI Platform
FIPS 140-2 Non-Proprietary Security Policy Level 2 Validation

Firmware Version: FP4.3

Hardware Version: GQS-G30CHASF-00 with tamper-evident labels 550-1211-001

Version 1.3

July 4, 2023

EDITOR

Author	Title
Xinyu Fang	System Architecture
Xifang Zhang	Hardware Engineer
Ruiqin Weng	Software Manager

Revision History

Version	Description	Date	By
0.1	Initial Version	09/23/2020	Xinyu Fang
1.0	First version	12/31/2020	Xinyu Fang Xifang Zhang Ruiqin Weng
1.1	Revision submitted to CMVP	04/07/2021	Xinyu Fang Xifang Zhang Ruiqin Weng
1.2	Responded to CMVP comments	01/28/2022	Xinyu Fang
1.3	Responded to CMVP comments	07/04/2023	Xinyu Fang

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 Purpose

This is a non-proprietary Security Policy for the Infinera Groove G30 DCI Platform (Groove G30) Cryptographic Module. This Security Policy describes how the cryptographic module meets the requirements for a FIPS 140-2 level 2 validation as specified in the FIPS 140-2 standard. This Security Policy is part of the evidence documentation package to be submitted to the validation lab.

FIPS 140-2 specifies the security requirements for a cryptographic module protecting sensitive information. Based on four security levels for cryptographic modules this standard identifies requirements in eleven sections. For more information about the standard, please visit http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

1.2 Scope

This Security Policy specifies the security rules under which the cryptographic module operates its major properties. It does not describe the requirements for the entire system, which makes use of the cryptographic module.

1.3 Security level

The module meets the overall requirements applicable to FIPS140-2 Security Level 2. In the individual requirement sections of FIPS 140-2, the following Security Level ratings are achieved:

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

Table 1 – Security level per FIPS 140-2 section

2 Cryptographic module specification

Groove G30 is an innovative stackable transport solution for cloud and data center networks that delivers 4.8 terabits of capacity throughput in a compact 1RU form factor. Groove G30 enables Wide Area Network (WAN) cloud connectivity services, including 10G, 40G, 100G, and 400G client services. Powered by Infinera CloudWave™ Optics, Groove G30 supports programmable DWDM line interface bandwidth and performance to optimize high-capacity transmission from 100G to 600G per wavelength in metro, regional, or long-haul DCI applications. As a key solution of Infinera Open Line System (OLS), ROADM (Reconfigurable Optical Add-Drop Multiplexer) provides reconfigurable multiplexing and de-multiplexing of wavelengths that are added, dropped, or passed through from one DWDM interface to up to three other DWDM interfaces. Groove™ G30 provides DWDM Optical Multiplexing/De-multiplexing, optical amplification, tunable dispersion compensation, optical time domain reflectometer, optical channel monitor, and protection with relevant Optical Cards.

The cryptographic module is a multi-chip standalone module. Groove™ G30 contains 1 controller card (Field Replaceable Control Unit (FRCU)) at slot 12, 4 universal service slots, slot-1, slot-2, slot-3 and slot-4. Each slot can support a single slot module. Slot 1 and slot 3 can support a dual slot module.

The module is validated with following versions:

- Firmware version: FP4.3
- Hardware version: GQS-G30CHASF-00 with tamper-evident labels 550-1211-001.

2.1 Cryptographic module boundary

The cryptographic boundary of module is defined as the entire shelf. And the extent of the cryptographic boundary is the outer metal chassis.

The module hardware model is shown as following:

Figure 1 – Front view of Groove G30 shelf with slot cards

Figure 2 – Back view of Groove G30 shelf

2.2 Hardware

The module is a multi-chip module that contains different kinds of cards. The cryptographic boundary of the multi-chip module is defined in section 2.1 of this document.

The cryptographic module is composed of the following components:

One Groove™ G30 chassis, five fan modules, two power modules, one Field Replaceable Control Unit (FRCU), and pluggable cards.

The pluggable cards include CHM1/CHM1LH, CHM1G, CHM2/CHM2LH, CHM2T, XTM2, OMD96, OMD48-S, OMD64, OCC2, RD09, UTM2, and CHM Filler Plate.

2.3 Mode of operation

The module has a FIPS Approved mode of operation and a FIPS non-Approved mode of operation.

The module will be placed into FIPS Approved mode of operation when “FIPS” mode is set. When “NONFIPS” mode is set, the module will be placed into FIPS non-Approved mode of operation.

Crypto Officers can set “FIPS” mode or “NONFIPS” mode by issuing CLI commands to the module.

The procedure and detail CLI commands are described in Section 11.4 Switching between FIPS Approved mode of operation and FIPS non-Approved mode of operation.

When the cryptographic module runs in FIPS Approved mode of operation and the Crypto Officer switches the module to FIPS non-Approved mode of operation, the CSPs will be zeroized automatically and the module will restart into FIPS non-Approved mode of operation.

When the cryptographic module runs in FIPS non-Approved mode of operation and the Crypto Officer switches the module to FIPS Approved mode of operation, the CSPs will be zeroized automatically and the module will restart into FIPS Approved mode of operation.

2.4 FIPS Approved security functions

The table below gives the list of FIPS Approved security functions that are provided by the module.

Algorithm	Certificate Number
AES-CBC-128/256, AES-CTR-128/256, AES-ECB-128/256 (OpenSSL)	CAVP Cert. #A651
AES-CBC-128/192/256, AES-CTR-128/192/256, AES-ECB-128/192/256 (Kernel crypto)	CAVP Cert. #A658
AES-CTR-256 AES-GMAC (key length:256 bits; tag length: 128 bits) *Note1* (Hardware encryption engine from vendor Microsemi Corporation)	CAVP Cert. #3844 (Certificate from hardware vendor)
AES-ECB-256 *Note 1* (Hardware encryption Engine from vendor Acacia Communications Inc.)	CAVP AES Cert. #4707 (Certificate from hardware vendor)
AES-GCM-256 *Note 1* (OpenSSL)	CAVP Cert. #A651
AES-GCM-256 *Note 1* (Kernel crypto)	CAVP Cert. #A658
AES-GCM-256 *Note1* (Hardware encryption Engine from vendor Acacia Communications Inc.)	CAVP AES Cert. #4770 (Certificate from hardware vendor)
AES-GCM-256 *Note1* (Hardware encryption Engine from vendor Acacia Communications Inc.)	CAVP Cert. #C646 Certificate from hardware vendor)
AES-KW-256*Note2* (OpenSSL)	CAVP Cert. #A651
CKG – IG D.12 [SP.800-133r2, 5.1] Key Pairs generation using unmodified DRBG output for Digital Signature Schemes [SP.800-133r2, 5.2] Key Pairs generation using unmodified DRBG output for Key Establishment [SP.800-133r2, 6.1] The "Direct Generation" of Symmetric Keys generation using unmodified DRBG output [SP.800-133r2, 6.2.1] Symmetric Keys Generated Using Key-Agreement Schemes [SP.800-133r2, 6.4] Distributing Symmetric Keys using key wrapping	Vendor Affirmed
Counter DRBG (AES-256) (OpenSSL)	CAVP Cert. #A651
ECDSA KeyGen (FIPS 186-4) Curve: P-224, P-256, P-384, P-521	CAVP Cert. #A651

Algorithm	Certificate Number
ECDSA KeyVer Curve: P-224, P-256, P-384, P-521 ECDSA SigGen Curve: P-224, P-256, P-384, P-521 Hash: SHA2-224, SHA2-256, SHA2-384, SHA2-512 ECDSA SigVer Curve: P-224, P-256, P-384, P-521 Hash: SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512 (OpenSSL)	
ENT (P)*Note 3*	N/A
HMAC-SHA-1-96/160, HMAC-SHA2-224, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512 (OpenSSL)	CAVP Cert. #A651
HMAC-SHA-1-96, HMAC-SHA2-224, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512 (Kernel crypto)	CAVP Cert. #A658
KAS-ECC Component: Ephemeral Unified: KAS Role: Initiator, Responder KDF without Key Confirmation: Parameter Set: EB: Hash Algorithm: SHA2-224, Curve: P-224 EC: Hash Algorithm: SHA2-256, Curve: P-256 ED: Hash Algorithm: SHA2-384, Curve: P-384 EE: Hash Algorithm: SHA2-512, Curve: P-521 KAS-FFC Component: dhEphem: KAS Role: Initiator, Responder KDF without Key Confirmation: Parameter Set: FB: Hash Algorithm: SHA2-224 FC: Hash Algorithm: SHA2-256 KAS-ECC-SSC (SP800-56Ar3): *Note 4* Domain Parameter Generation Methods: P-224, P-256, P-384, P-521 Scheme: ephemeralUnified: KAS Role: initiator, responder ((Cofactor) Ephemeral Unified Model, C(2e, 0s, ECC CDH) Scheme) KAS-FFC-SSC (SP800-56Ar3): *Note 4* Domain Parameter Generation Methods: FB, FC Scheme: dhEphem: KAS Role: initiator, responder	CAVP Cert. #A651

Algorithm	Certificate Number
(dhEphem, C(2e, 0s, FFC DH) Scheme) (OpenSSL)	
CVL – IKEv2 *Note 5* Capabilities: Initiator Nonce Length: 128-384 Responder Nonce Length: 128-384 Diffie-Hellman Shared Secret Length: 384 Derived Keying Material Length: 1056-2432 Hash Algorithm: SHA2-384 Capabilities: Initiator Nonce Length: 128-384 Responder Nonce Length: 128-384 Diffie-Hellman Shared Secret Length: 2048 Derived Keying Material Length: 1056-2432 Hash Algorithm: SHA-1, SHA2-256 (Kernel crypto)	CAVP Cert. #A658
CVL – SNMP *Note 5* Password Length: 64-96 (OpenSSL)	CAVP Cert. #A651
CVL – SSH *Note 5* Cipher: AES-128, AES-192, AES-256 Hash Algorithm: SHA-1, SHA2-224, SHA2-256, SHA2- 384, SHA2-512 (OpenSSL)	CAVP Cert. #A651
CVL – TLS *Note 5, Note 6* TLS Version: v1.2 Hash Algorithm: SHA2-256, SHA2-384 (OpenSSL)	CAVP Cert. #A651
RSA KeyGen (FIPS 186-4) Key Generation Mode: B.3.3 Modulo: 2048 Modulo: 3072 RSA SigGen Signature Type: ANSI X9.31 Modulo: 2048 with SHA2-256, SHA2-384, SHA2-512 Modulo: 3072 with SHA2-256, SHA2-384, SHA2-512 Modulo: 4096 with SHA2-256, SHA2-384, SHA2-512 Signature Type: PKCS 1.5 Modulo: 2048 with SHA2-256, SHA2-384, SHA2-512 Modulo: 3072 with SHA2-256, SHA2-384, SHA2-512 Modulo: 4096 with SHA2-256, SHA2-384, SHA2-512 RSA SigVer Signature Type: ANSI X9.31 Modulo: 2048 with SHA-1, SHA2-256, SHA2-384, SHA2-512 Modulo: 3072 with SHA-1, SHA2-256, SHA2-384, SHA2-512	CAVP Cert. #A651

Algorithm	Certificate Number
Signature Type: PKCS #1.5 Modulo: 2048 with SHA-1, SHA2-256, SHA2-384, SHA2-512 Modulo: 3072 with SHA-1, SHA2-256, SHA2-384, SHA2-512 (OpenSSL)	
SHA-1*Note 7*, SHA-224, SHA-256, SHA-384, SHA-512 (OpenSSL)	CAVP Cert. #A651
SHA-1 *Note 7*, SHA-224, SHA-256, SHA-384, SHA-512 (Kernel crypto)	CAVP Cert. #A658

Table 2 – FIPS Approved security functions

Note 1: The modules' AES-GCM implementation conforms to IG A.5 scenario #1 following RFC 7296 for IPSec/IKEv2, RFC 5288 for TLS, and RFC 5647 for SSHv2. The module's hardware encryption engine AES-GMAC and AES-GCM implementations conform to IG A.5, scenario #4.

Note 2: The key transport methods AES-KW is compliant to SP 800-38F according to IG D.9. The key establishment methodology provides 256 bits of encryption strength.

Note 3: The module implements SP800-90B compliant entropy source ENT (P). The entropy source falls into IG 7.14, Scenario #1a: A hardware module with an entropy-generating ENT (P) inside the module's cryptographic boundary. The hardware-based entropy source provides at least 256 bits of entropy to seed SP800-90A DRBG for the use of key generation.

Note 4: The module provides KAS-FFC-SSC and KAS-ECC-SSC compliant with SP 800-56Ar3, in accordance with Scenario X1 path (2) of IG D.8., combining KAS-SSC Cert. #A651 and CVL Cert. #C651 (KDF). KAS-FFC-SSC ([L, N] = [2048, 256] or [3072, 256]) provides 112 or 128 bits of encryption strength. And KAS-ECC-SSC (P-384) provides 192 bits of encryption strength. The module does not utilize non-56Arev3 functionality in the approved mode of operation.

Note 5: No parts of the [IKEv2, SSH, SNMPv3, and TLS] protocols, other than the KDF, have been tested by the CAVP or CMVP.

Note 6: The module supports the following TLS cipher suites allowed in section 3.3.1.1.1 and section 3.3.1.1.2 of SP 800-52 Rev 2:
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
The module doesn't support TLS cipher suites not allowed in SP 800-52 Rev 2.

Note 7: The module does not support individual SHA-1 service. SHA-1 is used in [IKEv2, SSH, SNMPv3, and TLS] protocols and digital signature verification (ECDSA and RSA).

Note 8: There are algorithms, modes, and keys that have been CAVP tested but not used by the module. Only the algorithms, modes/methods, and key lengths/curves/moduli shown in this table are used by the module.

2.6 FIPS non-Approved security functions

The module implements the following non-Approved algorithms which are not permitted for use in the FIPS 140-2 Approved mode of operation:

- MD5
- DES

2.7 Protocols allowed in Approved mode of operations

The module implements the following protocols which are permitted for use in the FIPS 140-2 mode

of operations:

- RADIUS over IPsec
- TACACS+ over IPsec

The allowed protocols in FIPS mode should be tunneled over an IPsec (cf. RFC 3162).

3 Cryptographic module ports and interfaces

The module provides a number of physical ports, and the physical ports can be categorized according to the following logical interfaces:

- Data Input Interface (DI)
- Data Output Interface (DO)
- Control Input Interface (CI)
- Status Output Interface (SO)
- Power Interface (Power)

Module	Name	Physical Ports	Qty.	Description	Logical Interfaces
Groove™ G30 Shelf Power Feeds	**PSUDC**	PWR A	1	Power A -48V input	Power
		PWR A RTN	1	Power A return	Power
		PWR B	1	Power B -48V input	Power
		PWR B RTN	1	Power B return	Power
	PSUAC	PWR A AC input	1	Power A input 110/220V	Power
		PWR B AC input	1	Power B input 110/220V	Power
	PSUHV	PWR A	1	Power A 240V input	Power
		PWR A RTN	1	Power A return	Power
		PWR B	1	Power B 240V input	Power
		PWR B RTN	1	Power B return	Power
Shelf Slot card (I/F) *Note1*	**CHM1/ CHM1LH**	CFP2-ACO	2	Optical connections	DI/DO/CI/SO
		QSFP28	4	Optical connections	DI/DO/CI/SO
	CHM1G	CFP2-ACO	2	Optical connections	DI/DO/CI/SO
		QSFP28	4	Optical connections	DI/DO/CI/SO
	CHM2/ CHM2LH	CFP2-ACO	2	Optical connections	DI/DO/CI/SO
		QSFP28/ QSFP+	10	Optical connections	DI/DO/CI/SO
	CHM2T	LC	4	Optical connections	DI/DO/CI/SO
		QSFP28	12	Optical connections	DI/DO/CI/SO
	XTM2	SFP+	20	Optical connections	DI/DO/CI/SO

Module	Name	Physical Ports	Qty.	Description	Logical Interfaces
		QSFP28	2	Optical connections	DI/DO/CI/SO
	UTM2	CFP2-DCO	2	Optical connections	DI/DO/CI/SO
		QSFP28	4	Optical connections	DI/DO/CI/SO
		SFP+	12	Optical module	DI/DO/CI/SO
Shelf Interface card (Optics) *Note1*	**OMD96**	LC	4	Optical connections	DI/DO/CI/SO
		MTP	24	Optical connections	DI/DO/CI/SO
	OMD48-S	MTP	12	Optical connections	DI/DO/CI/SO
		LC	4	Optical connections	DI/DO/CI/SO
	OMD64	LC	132	Optical connections	DI/DO/CI/SO
		RJ45	1	Connected to mini-USB of OCC2	DI/DO
		RJ45	1	Not functional	N/A
	OCC2	OFP2	3	Optical connections	DI/DO/CI/SO
		SFP	2	Optical connections	DI/DO/CI/SO
	RD09	LC	28	Optical connections	DI/DO/CI/SO
		SFP	1	Optical connections	DI/DO/CI/SO
		Type-C	1	Electrical interface	DI/DO/CI/SO
OFP2 Optical module installed on OCC2 *Note2*	**81.71T-O2PAOHIR-R6** **81.71T-O2PAOHLR-R6** **81.71T-O2PAOHER-R6**	LC	6	Optical connections	DI/DO/CI/SO
	81.71T-O2BAH-R6	LC	2	Optical connections	DI/DO/CI/SO
	ZXS-O2PAOULR-00	LC	5	Optical connections	DI/DO/CI/SO
	ZXS-O2BAUZZZ-00	LC	2	Optical connections	DI/DO/CI/SO
	81.71T-O2PAOSC-R6 **81.71T-O2PABA-R6**	LC	4	Optical connections	DI/DO/CI/SO
	ZXS-O2OMD8B1-00 **ZXS-O2OMD8B2-00** **ZXSO2CAD8ZZ-00** **ZXS-O2CAD8EZ-00**	LC	4	Optical connections	DI/DO/CI/SO
	ZXS-O2TDCMZZ-00	LC	1	Optical connections	DI/DO/CI/SO
	ZXS-O2OTDR4Z-00	LC	1	Optical connections	DI/DO/CI/SO
	ZXS-O2OPS1ZZ-00	LC	3	Optical connections	DI/DO/CI/SO
	ZXS-O2OCMZZZ-00	LC	4	Optical connections	DI/DO/CI/SO
Control Card	**FRCU** *Note 3*	RJ45	1	1000Base-T	DI/DO/CI/SO
		RS232	1	RS232 console	DI/DO/CI/SO
		USB	1	Not functional	N/A
		Pull Button	1	Press for pulling out FRCU	CI
		LED	1	Indicating FRUCU is ready for pull out. (red)	SO

Module	Name	Physical Ports	Qty.	Description	Logical Interfaces
		Reset Button	1	Press for 5 seconds to cold boot the module. Press for 30 seconds to reset the module to clear database, all provisions will be lost.	CI
Shelf interface	**N/A**	SD card socket	1	SD Card interface	DI/DO

Table 3 – Ports and logical Interfaces

Note 1: The "data input interface" and "control input interface" are different from "data output interface" and "status output interface" on message transmission direction. The fiber channels from the module to the outside are the "data output interfaces" and "control output interfaces". The fiber channels from the outside to the module are the "data input interfaces" and "control input interfaces". In a fiber channel, the control input interface or status output interface occupies the OH (overhead) bytes of the channel while data input interface or data output interface occupies the data bytes of the channel.

Note 2: These physical ports may include inband channels (OSC, GCC) for module management purpose, so "Control Input Interface" and "Status Output Interface" should be listed here.

Note 3: Groove™ G30 provides data encryption functions on FRCU cards.

4 Roles, services and authentication

The supported authorized roles, the services provided for those roles, and the related authentication mechanisms are covered in this section.

4.1 Authorized roles

The module supports two authorized roles: a CO (Crypto Officer) role and a User role. They are responsible for cryptographic module initialization, configuration, key management, status retrieve, etc. Detailed services provided for them are listed in the table in Services section.

The module have 5 user group levels, which are mapped to the CO role and User role as the below table. The users in crypto-officer and administration user groups are in the CO role. The users in configuration, operation and supervision user groups are in user role.

Authorized roles	User group	Access permissions
CO role	crypto-officer	The highest level of access privilege. Crypto-officer can do all of the operations that an administrator can do plus configurations related with ODU encryption.

	administration	The administrative users can perform all management operation including security.
User role	configuration	Configuration level users can support all management operations except for security related management operations.
	operation	Operation level users' privilege is between configuration and supervision level users', such as, 'ping' and 'traceroute'.
	supervision	Supervision level users can only do monitoring operation without the access to all configuration change operations.

Table 4 – Roles and User Groups

Multiple concurrent operators are allowed to this module. The maximum number of operators is 50, the maximum number of sessions is 100. They are identified and authorized by username and password. The multiple concurrent operators can be in CO role and in User role. But the module does not permit an operator to change roles.

The module does not support a Maintenance Role.

4.2 Services

The services for the authorized CO and User roles are listed in the table below.

The following indicators are used for showing the type of access required for the Critical Security Parameters (CSPs):

R – Read, the CSP is read.

W – Write, the CSP is established, generated, modified, or zeroized.

X – Execute, the CSP is used within an Approved or Allowed security function or authentication mechanism.

Service	CO	User	Description	Input	Output	CSP and Type of Access
Initialize the module	√	√	Initialize the module	Command	Status output	Master key – R/W/X
Configure and show the system	√	√	Configure and show system settings	Command and parameters	Command response	None
Set FIPS mode	√	√	Switch from FIPS-approved	Command	Command	Zeroize all plaintext

Service	CO	User	Description	Input	Output	CSP and Type of Access
			security function mode to FIPS-non approved security function mode	and parameters	response	CSPs
Show FIPS mode	√	√	Show current mode of operation	Command and parameters	Command response	None
Generate asymmetric key pair	√		Generate the asymmetric key pair for certificate and SSH	Command and parameters	Command response	ECDSA or RSA Private Key – W ECDSA or RSA Public Key – W
Manage CA certificate, root CA certificate and CRL	√		Generate CSR, Export CSR, Import signed CA certificate, Import root CA certificate, Import CRL	Command and parameters	Command response	Certificate private key and public key – R/X
Create data encryption / decryption service	√		Encrypt or decrypt user data, and manage the data encryption/decryption key	Command and parameters	Command response	Data encryption AES key – X
Manage TLS session for data traffic	√	√	Build up TLS session for data traffic	Command and parameters	Command response	TLS session Key – W/X
Monitor alarms	√	√	Monitor alarms for diagnostic purpose	Command	Status output	None
View system logs	√	√	View system status messages in historical alarm log and provisioning log	Command	Status output	None
Perform device diagnostics	√	√	Test the module during operation	Command and parameters	Command response and status via log and LEDs	None
Upgrade application firmware, FPGA image and chipset firmware *Note1*	√	√	Upgrade the application firmware, FPAG image and chipset firmware using RSA signature verification	Command and parameters	Command response and status output	RSA Public Key – X
IPsec	√		Secure, rekeying, communications between the module and Management system over DCN	Command and parameters	Command response and Status output	Certificate private key and public key – X Volatile, internal, generated, symmetric authentication and encryption keys with perfect forward secrecy - X
Zeroize	√		Zeroize the Master key	Command	Command response	Refer to the Section *11.2* for details
Perform on demand self-tests	√	√	Perform self-tests on demand	Command	Status output	None
Power on self-tests			Perform self-tests when system is power on; services not requiring an authorized role.	None	Status output	None

Service	CO	User	Description	Input	Output	CSP and Type of Access
Perform Packet Service	√	√	Perform packet related service provisioning and status retrieval.	Command	Command response	None
Perform L0 optical service	√	√	Perform L0 optical related service provisioning and status retrieval.	Command	Command response	None
Perform L1 OTN service	√	√	Perform L1 OTN related service provisioning and status retrieval.	Command	Command response	None
CLI	√	√	Access the module through Secure Shell (SSH)	Command	Command response	SSH keys and user credentials – R
Key Wrap	√		Wrap the key for ODU encryption key during synchronization to peer	None	Command response	ODU encryption key – R
SNMPv3	√	√	SNMPv3 service	Command	Command response	SNMP privacy and authentication passphrases – R
Diffie-Hellman	√	√	Provides 112 or 128 bits of encryption strength.	None	None	Shared secret-R/W/X
Elliptic Curve Diffie-Hellman	√	√	Provides 192 bits of encryption strength.	None	None	Shared secret-R/W/X
NDRNG			Provides 512 bits of random number to seed the DRBG. Services not requiring an authorized role.	None	None	Shared secret-W
RADIUS over IPsec	√	√	Remote User authentication	Command	Command response	Shared secret-R/X
TACACS+ over IPsec	√	√	Remote User authentication	Command	Command response	Shared secret-R/X
Telemetry	√	√	Status subscription	Command	Command response	Certificate private key and public key – R/X
WebGUI	√	√	Access the module through HTTPS	Command	Command response	Certificate private key and public key – R/X
RestConf	√	√	Access the module through HTTPS	Command	Command response	Certificate private key and public key – R/X
NetConf	√	√	Access the module through SSH	Command	Command response	SSH keys and user credentials – R
File Service	√	√	Access the file through SSH	Command	Command response	User credentials – R

Table 5 – FIPS Approved services

Note 1: Crypto Officer is the only role to conduct the firmware upgrade service. Prior to the firmware upgrade operation, the module shall perform the firmware load test by verifying the signature of the updated firmware image. Please note that the updated firmware shall be validated by CMVP prior to loading to maintain validation. For firmware load test, please refer to section 9.2 in this document.

Service	CO	User	Description	Input	Output	CSP and Type of Access
MD5	√	√	Message Digest used for RADIUS and SNMP protocol	None	None	None
DES	√	√	The SNMP privacy protocol	None	None	None

Table 6 – FIPS non-Approved services

4.3 Authentication

The module performs identity-based authentication. The module security consists of the user identifier and a password identifier. Both identifiers must be accurately entered to gain access to the system.

4.3.1 CO and user authentication

The operators must be authenticated by the cryptographic module before being allowed to access to services that require the assumption of an authorized role. The module authenticates operators using their user name and password. If the password for the operator is validated against the password in memory (encrypting the input password with AES-256 ECB, then comparing the result with the saved password in RAM), the operator is allowed to entry to execute its services.

The following rules apply for the password complexity:

- Password length must be between 8 and 32 characters.
- The following character types must be present:
  - Numeric character, lowercase alphabetical character, uppercase alphabetical character, special character (~!@#$%^&*_-+=`|\(){}[]:;<>,.?’/”)
- Previous 5 passwords must not be used.
- The password must not include more than 2 consecutive repetitions of the same character.
- UID (UserId) must not be contained in password (case insensitive).

If 5 integers, 1 lowercase alphabetical character, 1 uppercase alphabetical character, and 1 special character are used for an 8-character password, the probability of randomly guessing the correct sequence is 1 in 1,419,275,520(this calculation is based on the assumption that the typical standard American QWERTY computer keyboard has 10 Integer digits, 26 lowercase alphabetic characters, 26 uppercase alphabetical characters , and 32 special characters to choose from in total. The calculation should be10x9x9x9x9x26x26x32= 1,419,275,520).

Therefore, the associated probability of a successful random attempt is approximately 1 in 1,419,275,520, which is less than the 1 in 1,000,000 required by FIPS 140-2.

The login will be locked out for the operator (the period of the lockout is user defined, max 300

seconds, min 60 seconds, which can be set by Crypto Officer through CLI command ED-SECU-SYS), when the maximum number of consecutive and invalid attempts (maximum is 9) happen. So the associated probability of a successful random attempt during a one-minute period is less than $9/1,419,275,520 = 6.34126x10^{-9}$, which is less than one in 100,000.

When the login password is entered in the command, only one asterisk (*) appears on the screen, regardless of how many characters comprise the password.

The user login command will give error message for failed login, but will not return specific error codes that may give hints to persons attempting unauthorized access.

The user passwords are stored in SD card and RAM. The passwords in SD card will be cleared when system is zeroized. When the module is warm reboot, cold reboot, powered off and zeroized, the user passwords in RAM are cleared.

Before the module is initialized, it can only be accessed via serial interface and local craft interface. After the module is initialized, the serial interface will be covered.

4.3.2 SSH authentication

In FIPS mode, users login to the module with secure shell (SSH). The module works as SSH server. It supports user password based and key based SSH authentications. The public key used for authentication can either be ECDSA or RSA, yielding at least 112 bits of strength, assuming the smallest curve size P-224 or modulus size 2048 bit. The chance of a random authentication attempt falsely succeeding is: $1/2^{112}$ which is less than 1/1,000,000, $1.92 x10^{-34}$, which is much less than one in 1,000,000. As the same lockout mechanism, maximum 9 attempts in one-minute, the probability of a successful random attempt during a one-minute period is $9/2^{112}$, $1.73 x10^{-33}$, which is also much less than one in 100,000 that is required by FIPS 140-2.

5 Physical security

To operate in FIPS Approved mode the tamper-evident labels shall be installed on the shelf as shown in Appendix A.

After the shelf has been configured to meet FIPS 140-2 Level 2 requirements, the shelf cannot be accessed without indicating signs of tampering.

The multi-chip standalone cryptographic module includes the following physical security mechanisms:

- Production-grade components and production-grade opaque enclosure.

- Tamper-evident labels. Refer to "Procedure 2: Install the tamper-evident labels" of Appendix A for detailed instructions on tamper-evident label placement.
- Service cards are installed in slots of shelf.
- All unpopulated slots are equipped with filler cards.

The tamper-evident mechanism is described as following.

- **Tamper-evident labels**

Tamper-evident labels shall be installed for the module to operate in an Approved mode of operation.

Two sizes of tamper-evident labels are used, the 2.360 inch x 0.230 inch size and the 1.200 inch x 0.600 inch size (the two sizes of labels share one Infinera PN: 550-1211-001). The following graphics illustrate the tamper-evident labels, drawing in inches.

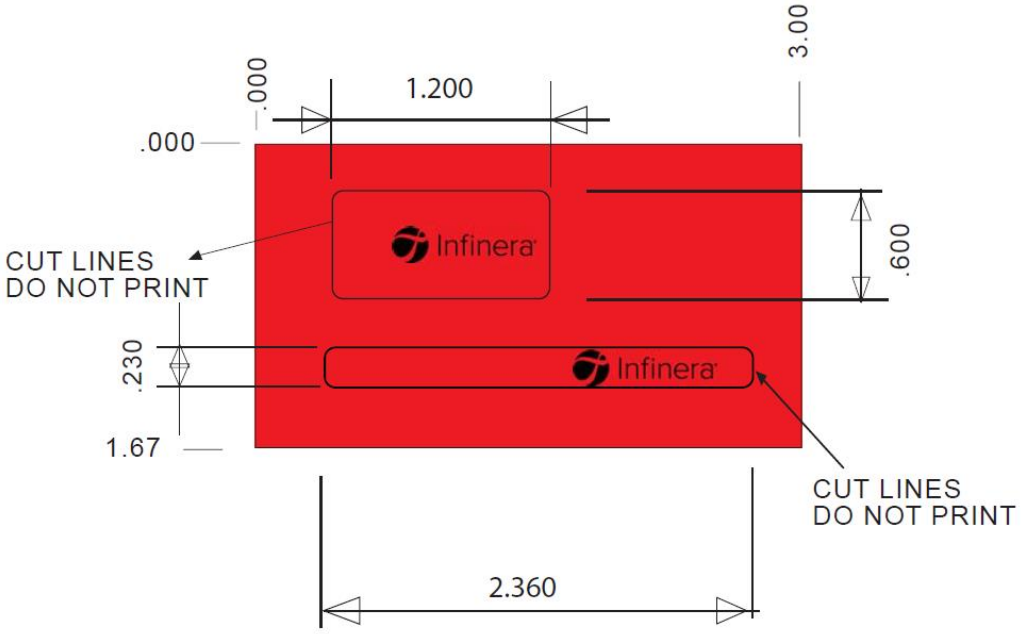

Figure 3 – Tamper-evident label

Figure 4, "Tamper-evident label: intact" illustrates a tamper-evident label with no evidence of tampering.

Figure 4 – Tamper-evident label: intact

Figure 5 – Tamper-evident label: broken

Figure 5, "Tamper-evident label: broken" illustrates a tamper-evident label that shows signs of tampering. Figure 6, "Tamper-evident label: broken (close-up view)" is a magnified view of the broken label. Note the VOID markings on the solid red label. If any portion of the VOID marking is visible, the equipment is showing signs of potential tampering.

Figure 6 – Tamper-evident label: broken (close-up view)

- **Inspect labels**

The Crypto Officer is also responsible for inspecting the tamper-evident labels on the shelves at least every 30 days. If any evidence of tampering is observed on the tamper-evident seals, the module

shall be considered to be in a non-compliant state.

Upon such discovery, the Crypto Officer should assume that the modules have been compromised and contact Infinera.

Detailed procedures on affixing labels is given in Appendix A.

6 Operational environment

The module does not contain a modifiable operational environment.

7 Cryptographic key management

The module has a set of cryptographic keys, cryptographic key components and CSPs. The plain text keys and CSPs can be zeroized by the Crypto Officer, and the zeroization operation will overwrite RAM that stores the temporary keys.

Each key entered into or output from the module is associated with one of the COs or with one of the users created by the CO. The module does not support manual key entry. Moreover, in order to comply with FIPS 140-2 standard requirements, all data output interfaces except the status output interface are inhibited during the key entry/output processes.

- Key storage and zeroization

The module has a Master key stored on the EEPROM of the system, which is initialized when the module is switched from FIPS non-Approved mode to FIPS Approved mode and zeroized automatically when the module is switched from FIPS Approved mode to FIPS non-Approved mode by the Crypto Officer. The Master key in the EEPROM will be rewritten to “all zero” when it is zeroized.

The module has plain text keys in the SRAM space on FPGA for the ODU encryption function. The keys will also be zeroized when the Crypto Officer manually zeroizes the keys or when the module is switched from FIPS Approved mode to FIPS non-Approved mode by the Crypto Officer.

All the other keys and CSPs are stored on the SD card and encrypted by Master key with AES-256 ECB algorithm.

- Random number

In the FIPS Approved mode of operation, the module uses SP800-90B compliant hardware RNG (NXP K82 chip) as entropy source ENT (P) to generate true random bits and sends them to DRBG as its seed. The DRBG uses the entropy source for instantiation and for periodic re-seeding. ENT (P) obtains 512-

bits of entropy for instantiation, and 512-bits of entropy for each re-seed. (According to SP800-90A, this can be considered as 256-bits of entropy and 256-bits of nonce) Therefore, the caveat "The module generates cryptographic keys whose strengths are modified by available entropy", as per IG 7.14, scenario 1a applies.

These seed values are temporarily stored in RAM and are zeroized by power cycling the module. These values are not accessible to any user. DRBG will feed random numbers to all the other cryptographic functions. The module implements SP 800-90A DRBG Section 11.3 Health tests.

- Key transportation

"ODU encryption AES-CTR key" and "ODU encryption AES-GMAC key" in the table below can be transported out of the module with AES-256 key wrap algorithm. The AES keys for key wrap are from the DH or ECDH key exchange between the module and its peers. Since keys being wrapped are keys of AES-CTR-256 and AES-GMAC-256, the cryptographic strength of the encryption key is equal to the cryptographic strength of the keys being wrapped.

- Key establishment

The module does not support manual key entry or intermediate key generation key output. The keys are electronically entered into and output from the module using a key transport method based on one of the key DH/ECDH establishment methods (as detailed in IG 7.7 that states "EXT CM Hardware to/from networked GPC", which qualifies as electronic distribution and electronic entry) detailed in the section above and ciphered with an AES 256 bits key which corresponds to the shared secret derived by DH/ECDH. DH/ECDH key agreement scheme compliant with SP800-56A Rev3 and IG D.8 scenario X1 (path 2) is used as part of the industrial protocols. The DH/ECDH KAS implements a shared secret computation with key derivation implemented by SP 800-135 KDF.

For example, during the TLS handshake, the keys that are entered or output to the module over the network, includes RSA/ECDSA public keys and the TLS pre-primary secret encrypted with RSA key only when using the RSA key exchange with TLS. For TLS with DH/ECDH key exchange, the TLS pre-primary secret is established during key agreement and is not output from the module. Once the TLS session is established, the TLS traffic is protected by AES encryption.

- Cryptographic key and critical security parameters

The module supports the following cryptographic keys, cryptographic key components, CSPs and Public keys.

Item	Usage	Generation	Output	Storage	Zeroization
IKEv2 HMAC	Session key integrity check (256 bits HMAC-SHA256;	Generated internally / key exchange	No output	RAM	Reboot Zeroization on rekeying

Item	Usage	Generation	Output	Storage	Zeroization
	384 bits HMAC-SHA384; 512 bits HMAC-SHA512)				
ESP HMAC	Session key Authentication (256 bits HMAC-SHA256; 384 bits HMAC-SHA384; 512 bits HMAC-SHA512)	Generated internally / key exchange	No output	RAM	Reboot Zeroization on rekeying
IKEv2 AES	Session key encryption (128 bits 256 bits)	Generated internally / key exchange	No output	RAM	Reboot Zeroization on rekeying
ESP AES	Session key Encryption (128 bits 256 bits)	Generated internally / key exchange	No output	RAM	Reboot Zeroization on rekeying
IPsec Pre Shared Secret	IKEv2 authentication (128 bits ~ 256 bits in HEX string)	Input by CLI command	No output	SD Card with AES encryption	FIPS/NONFIPS mode switching; Manual Zeroization; Power cycle Press reset button for 30s
Seed to DRBG	Used for function requiring random number (384 bits)	Generated internally by HW(K82)	No output	RAM	FIPS/NONFIPS mode switching; Manual Zeroization; Power cycle
DRBG V	Internal state values for the DRBG (128 bits)	Generated by DRBG	No output	RAM	FIPS/NONFIPS mode switching; Manual Zeroization; Power cycle
DRBG key	Internal state values for the DRBG (256 bits)	Generated by DRBG	No output	RAM	FIPS/NONFIPS mode switching; Manual Zeroization; Power cycle
Master key	Key to encrypt the other Key/CSP (256 bits)	Generated internally by DRBG	No output	EEPROM	FIPS/NONFIPS mode switching; Manual Zeroization
PID	User password (8 ~ 128 bytes string)	Input by CLI command	No output	SD Card with AES encryption	FIPS/NONFIPS mode switching; Manual Zeroization
Elliptic Curve Diffie-Hellman private key	Elliptic Curve Diffie-Hellman private key (p-384 curve; p-521 curve)	Generated internally	No output	RAM	FIPS/NONFIPS mode switching; Manual Zeroization; Power cycle
Elliptic Curve Diffie-Hellman public key	Elliptic Curve Diffie-Hellman public key (p-384 curve; p-521 curve)	Generated internally	output	RAM	FIPS/NONFIPS mode switching; Manual Zeroization; Power cycle
Elliptic Curve Diffie-Hellman shared secret	Elliptic Curve Diffie-Hellman shared secret (p-384 curve; p-521 curve)	Generated internally	No output	RAM	FIPS/NONFIPS mode switching; Manual Zeroization ;Power cycle
Diffie-Hellman private key	Diffie-Hellman private key (2048 bits; 3072 bits)	Generated internally	No output	RAM	FIPS/NONFIPS mode switching; Manual Zeroization; Power cycle
Diffie-Hellman public key	Diffie-Hellman public key (2048 bits; 3072 bits)	Generated internally	output	RAM	FIPS/NONFIPS mode switching; Manual Zeroization; Power cycle
Diffie-Hellman shared secret	Diffie-Hellman shared secret (2048 bits; 3072 bits)	Generated internally	No output	RAM	FIPS/NONFIPS mode switching; Manual Zeroization; Power cycle
TLS (DHE-RSA) preMaster secret	TLS preMaster secret	Derived from DH	No output	RAM	FIPS/NONFIPS mode switching; Manual Zeroization; Power cycle
TLS(DHE-RSA) Master Secret	TLS Master Secret (48 bytes)	Derived from DH	No output	RAM	FIPS/NONFIPS mode switching; Manual Zeroization; Power cycle
TLS(DHE-RSA) session key	TLS session key (128 bits; 256 bits)	Derived from DH	No output	RAM	FIPS/NONFIPS mode switching; Manual Zeroization; Power cycle
TLS(ECDHE-ECDSA) preMaster secret	TLS preMaster secret	Derived from ECDH	No output	RAM	FIPS/NONFIPS mode switching; Manual Zeroization; Power cycle
TLS(ECDHE-ECDSA) Master Secret	TLS Master Secret (48 bytes)	Derived from ECDH	No output	RAM	FIPS/NONFIPS mode switching; Manual Zeroization; Power cycle

Item	Usage	Generation	Output	Storage	Zeroization
TLS(ECDHE-ECDSA) session key	TLS session key (128 bits; 256 bits)	Derived from ECDH	No output	RAM	FIPS/NONFIPS mode switching; Manual Zeroization; Power cycle
System private Key for TLS and IPsec - RSA	System private Key – RSA (2048 bits; 3072 bits)	RSA Private key for generation of signatures, authentication and key establishment; Generated through command; Used to export CSR; Associated with NE certificate	No output	SD Card with AES encryption	FIPS/NONFIPS mode switching; Manual Zeroization
System public Key for TLS and IPsec - RSA	System public Key -RSA (2048 bits; 3072 bits)	Generated from System private Key in running time if requested by software functions	output	SD Card with AES encryption	FIPS/NONFIPS mode switching; Manual Zeroization
System private Key for TLS and IPsec - ECDSA	System private Key – ECDSA (256 bits; 384 bits; 521 bits)	ECDSA Private key for generation of signatures, authentication and key establishment; Generated through command; Used to export CSR; Associated with NE certificate	No output	SD Card with AES encryption	FIPS/NONFIPS mode switching; Manual Zeroization
System public Key for TLS and IPsec - ECDSA	System public Key – ECDSA (256 bits; 384 bits; 521 bits)	Generated from System private Key in running time if requested by software functions	output	SD Card with AES encryption	FIPS/NONFIPS mode switching; Manual Zeroization
TLS HMAC - SHA1	TLS HMAC (160 bits)	TLS integrity and authentication session keys	No output	RAM	FIPS/NONFIPS mode switching; Manual Zeroization; Power cycle
TLS HMAC - SHA384	TLS HMAC (384 bits)	TLS integrity and authentication session keys	No output	RAM	FIPS/NONFIPS mode switching; Manual Zeroization; Power cycle
SNMPv3 Privacy Passphrase	SNMPv3 Privacy secret (8 ~ 64 bytes string)	Input by CLI command	No output	SD Card with AES encryption	FIPS/NONFIPS mode switching; Manual Zeroization
SNMPv3 Authentication Passphrase	SNMPv3 Authentication secret (8 ~ 64 bytes string)	Input by CLI command	No output	SD Card with AES encryption	FIPS/NONFIPS mode switching; Manual Zeroization
SNMPv3 Privacy key	SNMPv3 Privacy Key (128 bits AES key)	Generated internally by Privacy passphrase	No output	RAM	FIPS/NONFIPS mode switching; Manual Zeroization; Power cycle
SNMPv3 Authentication key	HMAC SHA1 key (160 bits)	Generated internally by Authentication passphrase	No output	RAM	FIPS/NONFIPS mode switching; Manual Zeroization; Power cycle
ODU encryption AES-CTR key	ODU encryption AES-CTR key (256 bits)	Got from DRBG	wrapped by AES	RAM & SD Card with AES encryption	FIPS/NONFIPS mode switching; Manual Zeroization
ODU encryption AES-GMAC key	ODU encryption AES-GMAC key (256 bits)	Got from DRBG	wrapped by AES	RAM & SD card with AES encryption	FIPS/NONFIPS mode switching; Manual Zeroization
Key Wrap Key	Key Wrap Key for ODU encryption keys (256 bits)	Derived from DH or ECDH	No output	RAM	FIPS/NONFIPS mode switching; Manual Zeroization; Power cycle
SSHv2 server private key - ECDSA	SSH Key (256 bits; 384 bits; 521 bits)	Generated through command (ED-TCPIP)	No output	SD Card with AES encryption	FIPS/NONFIPS mode switching; Manual Zeroization
SSHv2 server public key - ECDSA	SSH public Key (256 bits; 384 bits; 521 bits)	Generated through command (ED-TCPIP)	output	SD Card with AES encryption	FIPS/NONFIPS mode switching; Manual Zeroization
SSHv2 server private key - RSA	SSH Key (2048 bits; 3072 bits)	Generated through command (ED-TCPIP)	No output	SD Card with AES encryption	FIPS/NONFIPS mode switching; Manual Zeroization;
SSHv2 server public key - RSA	SSH public Key (2048 bits; 3072 bits)	Generated through command (ED-TCPIP)	output	SD Card with AES encryption	FIPS/NONFIPS mode switching; Manual Zeroization
SSH session Key	SSH Encryption AES Key (128 bits AES key; 256 bits AES key)	Derived from DH/ECDH for AES-256/128-CBC/CTR/GCM	No output	RAM	FIPS/NONFIPS mode switching; Manual Zeroization; Power cycle
SSH authentication key	SSH authentication key used by message authentication function (256 bits for HMAC-SHA256;	Derived by SSH key agreement	No output	RAM	FIPS/NONFIPS mode switching; Manual Zeroization; Power cycle

Item	Usage	Generation	Output	Storage	Zeroization
	512 bits for HMAC-SHA512)				
RADIUS/TACACS+ shared secret	RADIUS shared secret (8 ~ 64 bytes string)	Input by CLI command	No output	SD Card with AES encryption	FIPS/NONFIPS mode switching; Manual Zeroization
CSR for TLS and IPsec (including System public Key) - ECDSA	CSR (including System public Key) – ECDSA (256 bits; 384 bits; 521 bits)	Generated from System private Key in running time if requested by software functions	output	RAM	FIPS/NONFIPS mode switching; Manual Zeroization; Power cycle
NE local certificate for TLS and IPsec(including System public Key) - ECDSA	NE local certificate (including System public Key) Key – ECDSA (256 bits; 384 bits; 521 bits)	Downloaded from external file server	No output	SD Card with AES encryption	FIPS/NONFIPS mode switching; Manual Zeroization
CSR for TLS and IPsec (including System public Key) - RSA	CSR (including System public Key) – RSA (2048 bits; 3072 bits)	Generated from System private Key in running time if requested by software functions	output	RAM	FIPS/NONFIPS mode switching; Manual Zeroization; Power cycle
NE local certificate for TLS and IPsec (including System public Key) - RSA	NE local certificate (including System public Key) – RSA (2048 bits; 3072 bits)	Downloaded from external file server	output	SD Card with AES encryption	FIPS/NONFIPS mode switching; Manual Zeroization
CA certificate for TLS and IPsec - RSA	CA certificate – RSA (2048 bits; 3072 bits)	Downloaded from external file server	No output	SD Card with AES encryption	FIPS/NONFIPS mode switching; Manual Zeroization
CA certificate for TLS and IPsec - ECDSA	CA certificate – ECDSA (256 bits; 384 bits; 521 bits)	Downloaded from external file server	No output	SD Card with AES encryption	FIPS/NONFIPS mode switching; Manual Zeroization
Data integrity check - public RSA key	Data integrity check - public RSA key (2048 bits)	hardcoded in the software image	No output	SD Card with AES encryption	N/A

Table 7 – Critical security parameters and public keys

8 Electromagnetic interference/compatibility (EMI/EMC)

The module was tested and found to be conformant to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (i.e., for business use).

9 Self-tests

The module performs both power-on and conditional self-tests. These tests are conducted automatically as part of the normal functions of the cryptographic module. They do not require any additional operator intervention. All data output via the data output interface will be inhibited when the power-up tests are performed.

If self-tests fail, the module will go into an error state and the FIPS_SELFTEST_FAIL alarm will be raised. In the error state, all data output via the data output interface will be inhibited.

9.1 Power-up self-tests

Each time this cryptographic module is powered up, it tests that the cryptographic algorithms still

operate correctly and that sensitive data have not been damaged. Restarting the cryptographic module provides a means by which the operator can perform the power-up self-tests on demand.

During power-up self-tests, data output is inhibited. After power-up self-tests succeed, data output will be resumed.

Power-up self-tests include:

- Algorithm self-tests
  - Linux Kernel
    - AES-ECB (128/256) Encrypt/Decrypt KAT
    - AES-CBC (128/256) Encrypt/Decrypt KAT
    - AES-GCM (256) Encrypt/Decrypt KAT
    - HMAC-SHA-1 | HMAC-SHA-224/256/384/512 KAT
    - IKEv2 KDF test
    - SHA-1 | SHA-224/256/384/512 KAT
  - OpenSSL
    - AES-ECB (128/256) Encrypt/Decrypt KAT
    - AES-CBC (128/256) Encrypt/Decrypt KAT
    - AES-GCM (256) Encrypt/Decrypt KAT
    - AES-KW KAT
    - DRBG KAT with health test
    - ECDSA P-256/384/521 with SHA-256/384/512 PCT
    - HMAC-SHA-1 / HMAC-SHA-224/256/384/512 KAT
    - KAS-ECC-SSC KAT: Per IG D.8 Scenario X1 – Primitive “Z” Computation with P-384 curve
    - KAS-FFC-SSC KAT: Per IG D.8 Scenario X1 – Primitive “Z” Computation with 2048-bit key
    - RSA Sign/Verify using 2048-bit key with SHA-256 KAT
    - SHA-1 | SHA-224/256/384/512 KAT
    - SNMP KDF test
    - SSH KDF test
    - TLS KDF test
  - ENT (P)
    - SP800-90B Start-Up health tests: Repetition Count Test (RCT) and Adaptive Proportion Test (APT)
- Software images integrity test with CRC32

  Integrity test is executed on main controller and each card when the software and/or firmware images are loaded.

9.2 Conditional self-tests

Conditional self-tests are performed while the conditions specified for following test occurs:

- RSA and ECDSA Pair-wise consistency test
  - RSA Pair-Wise Consistency Test
  - ECDSA Pair-Wise Consistency Test
- Software/firmware load integrity test with RSA signature
  - Any firmware loaded into this module that is not shown on the module certificate, is out of the scope of this validation and requires a separate FIPS 140-2 validation.
- Continuous random number generator test for DRBG
- Continuous random number generator test for ENT (P)
- ENT (P) SP800-90B compliant health tests: RCT and APT
- SP 800-90A DRBG Section 11.3 health test

If conditional self-tests fail, the module will disable the traffic by shutting down data output interface.

10 Mitigation of other attacks

The module does not claim to mitigate any other attacks.

11 Security operation

The module meets Level 2 requirements of FIPS 140-2. The sections below describe how to place and keep the module in the FIPS-approved security function mode of operation.

11.1 Initial setup

The Crypto Officer must follow the [*Groove™ G30 DCI Quick Installation Guide for FRCU Chassis*] and [*Groove™ G30 User Guide*] to have the initial setup.
(authorized customer can download the documents from technical support website: https://infinera.lightning.force.com/lightning/n/Downloads2)

Basic Commissioning is used to install a software load for Groove™ G30. Below is the preconditions and steps about basic commissioning.

- A serial cable (RS232 compliant) connecting from Groove™ G30 to serial terminal.
- A CAT5 Ethernet cable connecting from Groove™ G30 LCI interface to customer network.

- A FTP server which could be accessed from Groove™ G30's LCI interface to download the software image.

Steps:

1 Type 'uboot' in console terminal to stop the auto-boot. Use the default baud-rate 9600 for serial interface baud-rate.

2 Enter 'run bcmode' in the prompted uboot window, the system will reset to a linux prompt.

2.1 In bcmode, run:
/sbin/mkfs.ext4 /dev/sda1

2.2 Reboot by running:

2.2.1 mkdir /mnt/flashdisk

2.2.2 mount -t jffs2 -o ro,noatime /dev/mtdblock1 /mnt/flashdisk

2.2.3 /mnt/flashdisk/init_sys

2.3 Now the system restarted, type 'uboot' and enter 'run bcmode' in the prompted uboot window again.

3 mkdir /mnt/flashdisk

4 mount -t jffs2 -o ro,noatime /dev/mtdblock1 /mnt/flashdisk

5 cd /mnt/flashdisk

6 From the /mnt/flashdisk# prompt, enter the following commands to copy the SW image and execute:

6.1 /sbin/mkfs.ext4 /dev/sda1

6.2 ./bcm.init

6.3 ./ed_ip <NE ip address> <NE netmask> LCI <Gateway ip address>,
example of command: ./ed_ip 169.254.0.1 255.255.0.0 LCI 169.254.0.52

6.4 ./copy_rfile_ext4 <Remote FTP server ip address> 21 <FTP username> <FTP password> <SW load path> <SW load name>
example of command: ./copy_rfile_ext4 169.254.132.138 21 name1 passwd1 GROOVE_G30_4.2.0_20200805

6.5 ./install_sw

7 Copy the below files

cp /tmp/image/ActLoad.dcr /mnt/sdcard/images/offLoad.dcr

cp /tmp/image/ActLoad.zip /mnt/sdcard/images/offLoad.zip

8 Set node to FIPS mode with fipsmode=fips
./ed_sys [fipsmode=<fips|non-fips>]

9 Sync

10 ./init_sys

After system restarted, new software image starts to run.

For hardware setup, the Crypto Officer must follow the APPENDIX A Hardware procedures consistent with FIPS 140-2 user guide.

11.2 Manual zeroization

The Crypto Officer can zeroize the keys by perform CLI command "*clear-database clear-type=csp-zeroization*". The details of this command can be found in the [*Groove™ G30 CLI User Manual*].

The keys also can be zeroized by pressing reset button longer than 30s.

After the zeroization command is executed or the reset button is pressed longer than 30s, the Master key in the EEPROM will be zeroized, and the module will reboot automatically to clean the other keys in the RAM.

11.3 Switching between modes of operation

The Crypto Officer can switch the module between FIPS Approved mode and non-Approved mode of operation by executing CLI command "*security system-fips*".

In FIPS non-Approved mode of operation, the module will be switched to FIPS Approved mode of operation if the CLI command "*security system-fips*" is issued with parameter enabled.

In FIPS Approved mode of operation, the module will be switched to FIPS non-Approved mode of operation if the CLI command "*security system-fips*" is issued with parameter disabled.

Please note that when the module is switched between FIPS Approved mode and non-approved security function mode of operation, key zeroization and system restart will be automatically performed.

The current mode of operation can be retrieved by CLI command "*show system security system-fips*". Details of these two commands can be found in the [*Groove G30 User Guide*].

11.4 Key/IV Pair Uniqueness Requirements from SP 800-38D

There are three firmware AES-GCM implementations, one hardware AES-GMAC implementation on CHM2/CHM2LH/XTM2, and three hardware AES-GCM implementations on CHM1G and CHM2T.

The module's IPsec firmware AES-GCM implementation conforms to IG A.5, scenario #1. This IV generation of IPsec AES-GCM implementation is compliant with RFC 4106 and an IKEv2 protocol RFC7296 shall be used to establish the shared secret SKEYSEED from which the AES GCM encryption keys are derived. When the IV exhausts the maximum number of possible values for a given session key, the first party, client or server, to encounter this condition will trigger a handshake to establish

a new encryption key. The IPsec AES-GCM IV is only be used in the context of the AES GCM mode encryptions within the IPsec protocol. In case the Module's power is lost and then restored, the key used for IPsec AES-GCM shall be regenerated.

The module's TLS 1.2 firmware AES-GCM implementation conforms to IG A.5, scenario #1, following RFC 5288 for TLS. The counter portion of the IV is set by the module within its cryptographic boundary. When the IV exhausts the maximum number of possible values for a given session key, the first party, client or server, to encounter this condition will trigger a handshake to establish a new encryption key in accordance with RFC 5246. The TLS AES-GCM IV is only be used in the context of the AES GCM mode encryptions within the TLS protocol. In case the Module's power is lost and then restored, the key used for TLS 1.2 AES-GCM shall be regenerated.

The module's SSHv2 firmware AES-GCM implementation conforms to IG A.5, scenario #1. The SSHv2 implementation is compliant with RFC 4252 and RFC 4253 and the IV generation of SSHv2 AES-GCM implementation is compliant with RFC 5647. The SSHv2 AES-GCM IV is only be used in the context of the AES GCM mode encryptions within the SSHv2 protocol. In case the Module's power is lost and then restored, the key used for SSHv2 AES-GCM shall be regenerated.

The module's hardware (ODU encryption, CAVP Cert. #3844, CAVP AES Cert. #4707, CAVP AES Cert. #4770 and Cert. #C646) AES-GMAC/AES-GCM implementations conform to IG A.5, scenario #4. The hardware AES-GCM implementation uses a 96-bit IV, which is constructed deterministically per SP 800-38D Section 8.2.1 from a 32-bit nonce and a counter. The counter would not exceed its maximum value during the maximum configurable AES-GCM re-key interval (86400 seconds).

Per the requirements specified in Section 8 in NIST SP 800-38D, the probability that the authenticated encryption function ever will be invoked with the same IV and the same key on two (or more) distinct sets of input data is no greater than 2^{-32}. In case the Module's power is lost and then restored, the keys used for AES-GCM shall be regenerated.

12 References

[FIPS 140-2]	*Security Requirements for Cryptographic Modules* https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf
[FIPS 140-2 DTR]	*Derived Test Requirements for FIPS PUB 140-2, Security Requirements for Cryptographic Modules* https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/fips140-2/fips1402dtr.pdf
[FIPS 140-2 IG]	*Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program* https://csrc.nist.gov/csrc/media/projects/cryptographic-module-

validation-program/documents/fips140-2/fips1402ig.pdf

13 Acronyms

ACO	Alarm Cut Off
AES	Advanced Encryption Standard
APT	Adaptive Proportion Test
CA	Certificate Authority
CBC	Cipher Block Chaining
CFP	C Form-factor Pluggable
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CRC32	32-bit Cyclic Redundancy Check
CSP	Critical Security Parameter
CSR	Certificate Signing Request
DCC	Data Communication Channel
DCN	Data Communication Network
DES	Data Encryption Standard
DH	Diffie-Hellman
DRBG	Deterministic Random Bits Generator
DWDM	Dense Wavelength Division Multiplexing
ECB	Electronic Codebook Book
ECDSA	Elliptic Curve Digital Signature Algorithm
ECDH	Elliptic Curve Diffie-Hellman
ECDHE	Ephemeral Elliptic Curve Diffie-Hellman
EEROM	Electrically Erasable, Programmable Read Only Memory
EMC	Electromagnetic Compatibility
ENT (P)	Physical Entropy Source
EMI	Electromagnetic Interference

ESP	Encapsulating Security Payload
FCC	Federal Communication Commission
FIPS	Federal Information Processing Standard
FPGA	Field Programmable Gate Array
GCC	General Communication Channel
GCM	Galois/Counter Mode
GMAC	Galois Message Authentication Code
HMAC	Keyed-Hash Message Authentication Code
IP	Internet Protocol
IPsec	Internet Protocol Security
KAS	Key Agreement Schemes
KDF	Key Derivation Function
KTS	Key Transportation Schemes
LCI	Local Craft Interface
MD5	Message-Digest Algorithm
NDRNG	Non-deterministic Random number generators
ODU	Optical Data Unit
OFP1	Optical Form Factor Pluggable 1
OSC	Optical Supervisory Channel
OSM	OTN Switching Module
OTN	Optical Transport Network
PCT	Pair-Wise Consistency test
PID	Password ID
POL	Pluggable Optical Layer
PWR	POWER
RAM	Random Access Memory
RCT	Repetition Count Test
RNG	Random Number Generator
ROM	Read Only Memory

ROADM	Reconfigurable Optical Add-Drop Multiplexer
RSA	Rivest-Shamir-Adleman Public Key Algorithm
SAIM	Shelf Alarm Interface Module
SDM	Shelf Display Module
SD Card	Secure Digital Card
SEIM	Shelf Ethernet Interface Module
SFP	Small Form Pluggable
SFP+	Small Form Pluggable Plus
SHA	Secure Hash Algorithm
SPD	Security Policy Database
SNMP	Simple Network Management Protocol
SRAM	Static Random Access Memory
SSH	Secure Shell
STIM	Shelf Timing Interface Module
STPM	Shelf Timing and Processor Module
TRNG	True Random Number Generator
UID	User Identifier

APPENDIX A - Hardware procedures consistent with FIPS 140-2

Procedure 1: Install the Groove G30 FIPS kit

Purpose

The Infinera Groove G30 shelf requires tamper-evident labels to be FIPS compliant.

Refer to the [Groove G30 FP4.2 User Guide] for Groove G30 shelf installation guide.

Procedure 2: Install the tamper-evident labels

Purpose

Use this procedure to provide to install the tamper-evident labels on the module. Seal the systems only after you are sure that no additional provisioning/debugging is required. The tamper-evident label is shown in Figure 4.

Notes before tamper-evident labels installation

1. When applying tamper-evident labels, ensure that the surface temperature to be sealed is be a minimum of +10°F.
2. Ensure that the surface to be sealed is dry. Moisture of any kind can cause a problem. Wipe the area with a clean paper towel.
3. Ensure that the surface to be sealed is clean. Wipe the area with a clean cloth or paper towel to remove any dust or other loose particles.
4. If there are possible chemical contaminants (oil, lubricants, release agents, etc.), clean the surface with 100% iso-propyl alcohol. Wipe the alcohol dry with clean dry cloth or paper towel. **Note**: Avoid using rubbing alcohol; it can leave an oily coating that will interfere with adhesion of the label.
5. Installed tamper-evident labels shall be cured for 24 hours.

Steps

There are 15 tamper-evident labels to install on the module. Note that two sizes of 1.200 inch x 0.600 inch size label (SS, Short Size) and the 2.360 inch x 0.230 inch size label (LS, Long Size) share the same Infinera PN of 550-1211-001.

1. As shown in Figure 7, the operator shall install Label 1, 2, and 3 (3 pieces LS) on the top right side of the slot card or CHM Filler Plate and Label 4 (1 piece LS) on the top left side of the FRCU card.

For OCC2 slot card, Label 5, 6, and 7 (3 pieces LS)needs to be installed by covering the screws of the OFP2 or OFP2 Dummy plate. Install the label by covering the shelf if OCC2 slot card is inserted into slot1.

Figure 7 – Tamper-evident labels installation (Front view)

2. As shown in Figure 8, the operator shall install Label 8 and 9 (2 pieces LS) on the top left side of the 2 pcs of PSU card and Label 10, 11, 12, 13, and 14 (5 pieces SS) on the top center side of the 5 pcs of FAN card. Install Label 15 (1 piece SS) on rear right side of the shelf.

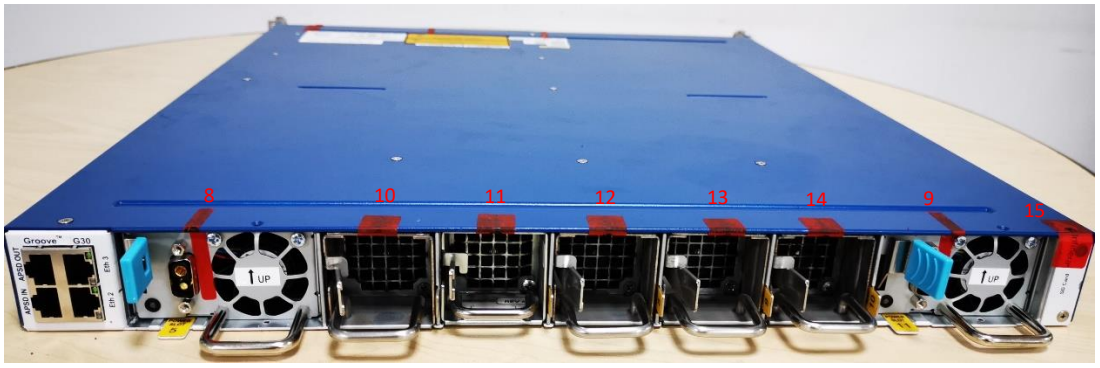

Figure 8 – Tamper-evident labels installation (Rear view)