



Infinera Corporation
Infinera Groove G30 Cryptographic Module
Version 4.6.6

FIPS 140-3 Non-Proprietary Security Policy

Document Version: 1.7
Last update: 09-24-2026

Table of Contents

1 General	4
1.1 Overview	4
1.2 Security Levels	4
2 Cryptographic Module Specification	4
2.1 Description	4
2.2 Tested and Vendor Affirmed Module Version and Identification	9
2.3 Excluded Components	10
2.4 Modes of Operation	10
2.5 Algorithms	12
2.6 Security Function Implementations	18
2.7 Algorithm Specific Information	21
2.8 RNG and Entropy	22
2.9 Key Generation	22
2.10 Key Establishment	23
2.11 Industry Protocols	23
3 Cryptographic module interfaces	23
3.1 Ports and Interfaces	23
4 Roles, services, and authentication	25
4.1 Authentication Methods	25
4.1.1 Password-based authentication	26
4.1.2 Public key based SSH authentication	27
4.2 Roles	27
4.3 Approved Services	28
4.4 Non-Approved Services	44
4.5 External Software/Firmware Loaded	44
5 Software/Firmware security	44
5.1 Integrity Techniques	44
5.2 Initiate on Demand	44
6 Operational environment	44
7 Physical security	45
8 Non-invasive security	45
9 Sensitive security parameters management	45
9.1 Storage Areas	45
9.2 SSP Input-Output Methods	46
9.3 SSP Zeroization Methods	46

9.4 SSPs	47
9.5 Transitions	60
10 Self-tests	60
10.1 Pre-operational self-tests	60
10.2 Conditional self-tests	61
10.3 Periodic Self-Test Information	66
10.4 Error States	68
11 Life-cycle assurance	68
11.1 Installation, Initialization, and Startup Procedures	68
11.2 Administrator Guidance	71
11.3 Non-Administrator Guidance	71
11.4 End of Life	71
12 Mitigation of other attacks	71

List of Tables

Table 1: Security Levels	4
Table 2: Tested Module Identification – Hardware	9
Table 3: Slot cards on the Cryptographic Module	10
Table 4: Modes List and Description	11
Table 5: Approved Algorithms	16
Table 6: Vendor-Affirmed Algorithms	17
Table 7: Non-Approved, Not Allowed Algorithms	17
Table 8: Security Function Implementations	21
Table 9: Entropy Certificates	22
Table 10: Entropy Sources	22
Table 11: Ports and Interfaces	25
Table 12: Authentication Methods	26
Table 13: Roles	27
Table 14: Approved Services	44
Table 15: Non-Approved Services	44
Table 16: Storage Areas	45
Table 17: SSP Input-Output Methods	46
Table 18: SSP Zeroization Methods	46
Table 19: SSP Table 1	54
Table 20: SSP Table 2	60
Table 21: Pre-Operational Self-Tests	60
Table 22: Conditional Self-Tests	65
Table 23: Pre-Operational Periodic Information	66
Table 24: Conditional Periodic Information	68
Table 25: Error States	68

List of Figures

Figure 1 – Front, rear, and side views of G30 chassis	6
Figure 2 – Front, rear, and side views of G30 chassis with sliding rails	7
Figure 3 – Front, rear, and side views of G30 Field Replaceable Controller Unit (FRCU) chassis	8

1 General

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for version FP4.6.6 of Infinera Groove G30 Cryptographic Module. It contains the security rules under which the module must operate and describes how this module meets the requirements specified in FIPS PUB 140-3 (Federal Information Processing Standards Publication 140-3) for an overall Security Level 1 module.

1.2 Security Levels

Section	Title	Security Level
1	General	1
2	Cryptographic module specification	1
3	Cryptographic module interfaces	1
4	Roles, services, and authentication	3
5	Software/Firmware security	1
6	Operational environment	1
7	Physical security	1
8	Non-invasive security	N/A
9	Sensitive security parameter management	1
10	Self-tests	1
11	Life-cycle assurance	1
12	Mitigation of other attacks	N/A
	Overall Level	1

Table 1: Security Levels

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

Infinera Groove G30 Cryptographic Module 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. Infinera Groove G30 Cryptographic Module enables Wide Area Network (WAN) cloud connectivity services, including 10G, 40G, 100G, and 400G client services. Infinera Groove G30 Cryptographic Module 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. Infinera Groove G30 Cryptographic Module provides DWDM Optical Multiplexing/De-multiplexing, optical amplification, tunable dispersion compensation, optical time domain reflectometer, optical channel monitoring, and protection with relevant Optical Cards.

Module Type: Hardware

Module Embodiment: Multi-Chip Standalone

Cryptographic Boundary:

The cryptographic boundary of the module is defined as the entire shelf. The extent of the cryptographic boundary is the outer metal chassis. There are three types of chassis for Infinera Groove G30 Cryptographic Module:

GQS-G30CHASZ-00 G30 chassis

GQS-G30CHASR-00 G30 chassis with sliding rails

GQS-G30CHASF-00 G30 Field Replaceable Controller Unit (FRCU) chassis

The module hardware models are shown as follows:



Figure 1 – Front, rear, and side views of G30 chassis



Figure 2 – Front, rear, and side views of G30 chassis with sliding rails



Figure 3 – Front, rear, and side views of G30 Field Replaceable Controller Unit (FRCU) chassis

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
GQS-G30CHASZ-00	Rev.A / Rev.B / Rev.C / Rev.D01	4.6.6	NXP QorIQ® P-2040 with PowerPC e500mc cores	G30 chassis
GQS-G30CHASR-00	Rev.A / Rev.B / Rev.C01 / Rev.D01	4.6.6	NXP QorIQ® P-2040 with PowerPC e500mc cores	G30 chassis with sliding rails
GQS-G30CHASF-00	Rev.A / Rev.B	4.6.6	NXP QorIQ® P-2040 with PowerPC e500mc cores	G30 Field Replaceable Controller Unit (FRCU) chassis

Table 2: Tested Module Identification – Hardware

Part Number	Product description
FRCU, Power, Fan, and Filler cards	
GCS-G30FRCUZ-00	G30 field replaceable controller unit (FRCU)
GPS-G30PSUAC-00	G30 110V/220V AC power module
GPS-G30PSUDC-00	G30 48V DC power module
GPS-G30PSUHV-00	G30 240V DC power module
GFS-G30FANZZ-00	G30 fan module
GLS-G30CHMFI-00	G30 CHM filler plate
OMD (Optical Multiplexing/Demultiplexing) cards	
GLS-G30OMD96-00	G30 OMD96
GLS-G30OMD48-SG	G30 OMD48 (standard grid)
L0 (Layer 0) cards	
GLS-G2RD09SM-N0	G30 1x9 ROADM
GLS-G30OCC2Z-00	G30 OCC2
81.71T-O2PAOSC-R6	OF2 PREAMP WITH OSC
81.71T-O2PABA-R6	OF2 PRE-AMP AND BOOSTER AMP
81.71T-O2PAOHIR-R6	IR Preamp + OSC Add/Drop, High Channel Count OF2
81.71T-O2PAOHLR-R6	LR Preamp + OSC Add/Drop, High Channel Count OF2
81.71T-O2PAOHER-R6	ER Preamp + OSC Add/Drop, High Channel Count OF2
81.71T-O2BAH-R6	Booster Amplifier OF2 (BA OF2), High Channel Count
ZXS-O2OMD8B1-00	OF2 OMD8 Band 1
ZXS-O2OMD8B2-00	OF2 OMD8 Band 2
ZXS-O2TDCMZZ-00	TDCM (Tunable Dispersion Compensation Module) OF2
ZXS-O2BAUZZZ-00	OF2 BOOSTER AMP ULTRA HIGH POWER
ZXS-O2PAOULR-00	OF2 PREAMP ULTRA HIGH POWER LONGER REAC
ZXS-O2OPS1ZZ-00	OF2 1CH OPS MODULE
ZXS-O2OPS1PT-00	OF2 1CH OPS MODULE with PILOT TONE (O2OPSPT)
ZXS-O2OTDR4Z-00	OF2 OTDR 4-PORT
ZXS-O2OCMZZZ-00	OF2 OPTICAL CHANNEL MONITOR
ZXS-O2CAD8ZZ-00	OF2 CAD8 Colorless Add/Drop
ZXS-O2CAD8EZ-00	OF2 CAD8E Colorless Add/Drop Expandable

Part Number	Product description
ZXS-O2WS04SZ-00	OFP2 WSS 1x4 Single WSS
ZXS-O2CAD16A-00	OFP2 CAD 1x16 WITH AMPLIFIER
ZXS-O2BAXZZZ-00	OFP2 BOOSTER AMP HIGH CH EXTENDED GAIN
L1 (Layer 1) cards	
GLS-G30CHM1Z-00	G30 CHM1 (4x100G)
GLS-G30CHM2Z-00	G30 CHM2 (40x10G, 10x40G, 4x100G)
GLS-G30CHM2Z-NC	G30 CHM2 (40x10G,10x40G,4x100G, no enc)
GLS-G30CHM1L-00	G30 CHM1LH (4x100G)
GLS-G30CHM2L-00	G30 CHM2L (40x10G, 10x40G, 4x100G)
GLS-G30CHM1G-00	G30 CHM1G (4x100G)
GLS-G30CHM1G-NC	G30 CHM1G (4x100G, no enc)
GLS-CHM2TMTZ-01	CHM2T for line rates from 200G to 600G
GLS-CHM2TLHZ-01	CHM2T meeting <=400G line side spec
GLS-CHM2TSMZ-01	CHM2T "Super Metro" supports up to 600G line rate
GLS-G30XTM2Z-00	G30 XTM2
GLS-G30XTM2C-00	G30 XTM2 (WITH ENCRYPTION)
GLS-G30UTM2Z-00	G30 UTM2

Table 3: Slot cards on the Cryptographic Module

Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets):

N/A for this module.

Tested Module Identification – Hybrid Disjoint Hardware:

N/A for this module.

Tested Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

2.3 Excluded Components

There are no excluded components for the module.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
FIPS mode	Normal Operation with only approved services and security functions available	Approved	The operation mode can be retrieved by CLI, NETCONF, and WebGUI. The

Mode Name	Description	Type	Status Indicator
			system-fips attribute is displayed as enabled in FIPS mode.
Non-FIPS mode	Non-approved security functions are available	Non-Approved	The operation mode can be retrieved by CLI, NETCONF, and WebGUI. The system-fips attribute is displayed as disabled in Non-FIPS mode.

Table 4: Modes List and Description

The module has a FIPS approved mode of operation and a FIPS non-approved mode of operation. The module will be set in FIPS approved mode of operation when the FIPS mode is configured. When the non-FIPS mode is configured, the module will be set in 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 the FIPS non-approved mode of operation, the Sensitive Security Parameters (SSPs) will be zeroized automatically and the module will restart into the 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 the FIPS approved mode of operation, the SSPs will be zeroized automatically and the module will restart into the FIPS approved mode of operation.

Mode Change Instructions and Status:

Crypto Officers can set “FIPS” mode or “NON-FIPS” mode by issuing CLI commands to the module. The procedure and detailed operations are described in Section [11.1 Installation, Initialization, and Startup Procedures](#).

The indicator of the mode of operation is an attribute named **system-fips** which can be retrieved by CLI, NETCONF, or WebGUI. The **system-fips** attribute is displayed as *enabled* in FIPS mode and *disabled* in non-FIPS mode.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A5078	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC	A5112	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CTR	A5078	Direction - Decrypt, Encrypt Key Length - 128, 192, 256 Payload Length - Payload Length: 128 Supports Counter larger than maximum value - Yes Incremental Counter - Yes Counter Tests Performed - Yes	SP 800-38A
AES-CTR	A5112	Direction - Decrypt, Encrypt Key Length - 128, 192, 256 Payload Length - Payload Length: 128 Supports Counter larger than maximum value - Yes Incremental Counter - Yes Counter Tests Performed - Yes	SP 800-38A
AES-CTR	AES 3844	Key Length - 256 Counter Source - Internal	SP 800-38A
AES-ECB	A5078	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A5112	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	AES 4707	Direction - Encrypt Key Length - 256	SP 800-38A
AES-GCM	A5078	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256 Tag Length - 128, 64, 96 IV Length - IV Length: 96 Payload Length - Payload Length: 128, 136, 248, 256 AAD Length - AAD Length: 0, 128, 136, 248, 256	SP 800-38D
AES-GCM	A5112	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256 Tag Length - 128, 64, 96 IV Length - IV Length: 96, 128 Payload Length - Payload Length: 128, 136, 248, 256 AAD Length - AAD Length: 0, 128, 136, 248, 256	SP 800-38D
AES-GCM	AES 4770	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 256	SP 800-38D

Algorithm	CAVP Cert	Properties	Reference
		Tag Length - 128 IV Length - IV Length: 96	
AES-GCM	C646	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 256 Tag Length - 128 IV Length - IV Length: 96 Payload Length - Payload Length: 121856 AAD Length - AAD Length: 0	SP 800-38D
AES-GMAC	AES 3844	Direction - Decrypt, Encrypt Key Length - 256 Tag Length - 128 IV Length - IV Length: 96 AAD Length - AAD Length: 128	SP 800-38D
AES-KW	A5112	Direction - Decrypt, Encrypt Cipher - Cipher Key Length - 256 Payload Length - Payload Length: 128, 192, 256, 320, 4096	SP 800-38F
Counter DRBG	A5112	Prediction Resistance - Yes Supports Reseed - Yes Mode - AES-256 Derivation Function Enabled - No Additional Input - Additional Input: 0-384 Increment 192 Entropy Input - Entropy Input: 384 Nonce - Nonce: 0 Personalization String Length - Personalization String Length: 0-384 Increment 192 Returned Bits - 512	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-5)	A5112	Curve - P-224, P-256, P-384, P-521 Secret Generation Mode - testing candidates	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A5112	Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-5
ECDSA SigVer (FIPS186-4)	A5112	Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
ECDSA SigVer (FIPS186-5)	A5112	Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-5
HMAC-SHA-1	A5078	MAC - MAC: 96 Key Length - Key Length: 128-512 Increment 128	FIPS 198-1

Algorithm	CAVP Cert	Properties	Reference
HMAC-SHA-1	A5112	MAC - MAC: 96-160 Increment 32 Key Length - Key Length: 128-512 Increment 192	FIPS 198-1
HMAC-SHA2-224	A5112	MAC - MAC: 128-224 Increment 32 Key Length - Key Length: 128-512 Increment 192	FIPS 198-1
HMAC-SHA2-256	A5078	MAC - MAC: 128-256 Increment 128 Key Length - Key Length: 128-512 Increment 128	FIPS 198-1
HMAC-SHA2-256	A5112	MAC - MAC: 256 Key Length - Key Length: 128-512 Increment 192	FIPS 198-1
HMAC-SHA2-384	A5078	MAC - MAC: 384 Key Length - Key Length: 384-1024 Increment 320	FIPS 198-1
HMAC-SHA2-384	A5112	MAC - MAC: 384 Key Length - Key Length: 384-1024 Increment 320	FIPS 198-1
HMAC-SHA2-512	A5078	MAC - MAC: 512 Key Length - Key Length: 512-1024 Increment 256	FIPS 198-1
HMAC-SHA2-512	A5112	MAC - MAC: 512 Key Length - Key Length: 512-1024 Increment 256	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A5112	Domain Parameter Generation Methods - P-224, P-256, P-384, P-521 Hash Function Z - SHA2-512 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KAS-FFC-SSC Sp800-56Ar3	A5112	Domain Parameter Generation Methods - FB, FC, ffdhe2048, ffdhe3072, ffdhe4096, modp-2048, modp-3072, modp-4096 Hash Function Z - SHA2-512 Scheme - dhEphem - KAS Role - initiator, responder	SP 800-56A Rev. 3
KDF IKEv2 (CVL)	A5112	Initiator Nonce Length - Initiator Nonce Length: 128-384 Increment 256 Responder Nonce Length - Responder Nonce Length: 128-384 Increment 256 Diffie-Hellman Shared Secret Length - Diffie-Hellman Shared Secret Length: 384-2048 Increment 1664 Derived Keying Material Length - Derived Keying Material Length: 1056-2432 Increment 1376 Hash Algorithm - SHA-1, SHA2-256, SHA2-384	SP 800-135 Rev. 1
KDF SNMP (CVL)	A5112	Password Length - Password Length: 64, 96 Engine ID - 8000a4f50430343a63303a39633a63393a38623a3036	SP 800-135 Rev. 1
KDF SSH (CVL)	A5112	Cipher - AES-128, AES-192, AES-256 Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
RSA KeyGen (FIPS186-5)	A5112	Key Generation Mode - probableWithProbableAux Modulo - 2048, 3072, 4096 p mod 8 - 0 Primality Tests - 2powSecStr	FIPS 186-5

Algorithm	CAVP Cert	Properties	Reference
		q mod 8 - 0 Info Generated By Server - Yes Private Key Format - standard Public Exponent Mode - random	
RSA SigGen (FIPS186-5)	A5112	Hash Pair - Hash Algorithm - SHA2-256 Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5	FIPS 186-5
RSA SigVer (FIPS186-4)	A5112	Signature Type - ANSI X9.31, PKCS 1.5 Modulo - 2048, 3072, 4096 Hash Pair - Hash Algorithm - SHA-1 Public Exponent Mode - Random	FIPS 186-4
RSA SigVer (FIPS186-5)	A5112	Hash Pair - Hash Algorithm - SHA2-256 Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5 Public Exponent Mode - random	FIPS 186-5
Safe Primes Key Generation	A5112	Safe Prime Groups - ffdhe2048, ffdhe3072, ffdhe4096, modp-2048, modp-3072, modp-4096	SP 800-56A Rev. 3
Safe Primes Key Verification	A5112	Safe Prime Groups - ffdhe2048, ffdhe3072, ffdhe4096, modp-2048, modp-3072, modp-4096	SP 800-56A Rev. 3
SHA-1	A5078	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4
SHA-1	A5112	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4
SHA2-224	A5112	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4
SHA2-256	A5078	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4
SHA2-256	A5112	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4
SHA2-384	A5078	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4
SHA2-384	A5112	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4
SHA2-512	A5078	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4
SHA2-512	A5112	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4
SHA3-256	A5078	Message Length - Message Length: 0-65536 Increment 8	FIPS 202
SHA3-256	A5148	Message Length - Message Length: 0-65536 Increment 8	FIPS 202
TLS v1.2 KDF	A5112	Hash Algorithm - SHA2-256, SHA2-384 Key Block Length - Key Block Length: 1024	SP 800-135 Rev. 1

Algorithm	CAVP Cert	Properties	Reference
RFC7627 (CVL)			
TLS v1.3 KDF (CVL)	A5112	HMAC Algorithm - SHA2-256, SHA2-384 KDF Running Modes - DHE, PSK-DHE	SP 800-135 Rev. 1

Table 5: Approved Algorithms

Note 1: The module's firmware AES-GCM implementation conforms to IG C.H 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 C.H, scenario #4. Refer to [2.7 Algorithm Specific Information](#) for details.

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

Note 3: The module provides KAS-FFC-SSC and KAS-ECC-SSC compliant with SP 800-56Ar3, in accordance with Scenario 2 path (2) of IG D.F., combining KAS-SSC Cert. #A5112 and KDF Cert. #A5112 (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 4: No parts of the [IKEv2, SSH, SNMPv3, and TLS] protocols, other than the KDF, have been validated by the CAVP or CMVP.

Note 5: The module supports the following TLS cipher suites allowed in section 3.3.1.1.1, section 3.3.1.1.2, and section 3.3.1.2 of SP 800-52 Rev 2:

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
 TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
 TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
 TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
 TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
 TLS_AES_256_GCM_SHA384
 TLS_AES_128_GCM_SHA256

The module does not support TLS cipher suites not allowed in SP 800-52 Rev 2.

Note 6: 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 7: There are algorithms, modes, and keys that have been validated by CAVP 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.

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
CKG	Algorithm: AES / ECDSA Key Type: Symmetric and Asymmetric	N/A	[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

Name	Properties	Implementation	Reference
			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 [IG D.H] Requirements for Vendor Affirmation to SP 800-133

Table 6: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

Non-Approved, Not Allowed Algorithms:

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

Name	Use and Function
MD5	Authentication protocol of SNMPv3
DES	Privacy protocol of SNMPv3

Table 7: Non-Approved, Not Allowed Algorithms

These non-Approved algorithms are offered in FIPS non-approved mode of operation.

Protocols allowed in Approved Mode of Operations:

The module implements the following protocols which are permitted for use in the FIPS 140-3 mode of operations:

- RADIUS over IPsec
- TACACS+ over IPsec

The allowed protocols in FIPS mode should be tunneled over an IPsec connection.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
Authenticated Decryption	BC-Auth	Block cipher in AEAD(authenticated encryption with associated data) methods		AES-GCM: (A5078, A5112, AES 4770, C646) Key size: 128, 192, 256 AES-GMAC: (AES 3844) Key size: 128, 192, 256
Authenticated Encryption	BC-Auth	Block cipher in AEAD(authenticated encryption with associated data) methods		AES-GCM: (A5078, A5112, AES 4770, C646) Key size: 128, 192, 256 AES-GMAC: (AES 3844) Key size: 128, 192, 256
Decryption	BC-UnAuth	Block Cipher		AES-ECB: (A5078, A5112, AES 4707) Key size: 128, 192, 256 AES-CTR: (A5078, A5112, AES 3844) Key size: 128, 192, 256 AES-CBC: (A5078, A5112) Key size: 128, 192, 256
Encryption	BC-UnAuth	Block Cipher		AES-ECB: (A5078, A5112, AES 4707) Key size: 128, 192, 256 AES-CTR: (A5078, A5112, AES 3844) Key size: 128, 192, 256 AES-CBC: (A5078, A5112)

Name	Type	Description	Properties	Algorithms
				Key size: 128, 192, 256
KTS-KeyWrap	KTS-Wrap	Key Wrapping and unwrapping	IG D.G:approved or allowed method from IG D.G Caveat:Key establishment methodology provides 256 bits of security strength	AES-KW: (A5112) Key size: 128, 256
Message Authentication	MAC	Message Authentication generation		HMAC-SHA-1: (A5078, A5112) HMAC-SHA2-224: (A5112) HMAC-SHA2-256: (A5078, A5112) HMAC-SHA2-384: (A5078, A5112) HMAC-SHA2-512: (A5078, A5112)
Message Digest	SHA	Message Digest		SHA-1: (A5078, A5112) SHA2-224: (A5112) SHA2-256: (A5078, A5112) SHA2-384: (A5078, A5112) SHA2-512: (A5078, A5112) SHA3-256: (A5078, A5148)
RNG	CKG	Random number generation		Counter DRBG: (A5112) Mode: AES-256
Key pair generation	AsymKeyPair- KeyGen CKG	Key pair generation		ECDSA KeyGen (FIPS186-5): (A5112) ECDSA KeyGen (FIPS186-5): P-224, P-256, P-

Name	Type	Description	Properties	Algorithms
				384, P-521, SHA2-224, SHA2-256, SHA2-384, SHA2-512 RSA KeyGen (FIPS186-5): (A5112) RSA KeyGen (FIPS186-5): 2048, 3072, 4096, SHA2- 256, SHA2-384, SHA2-512 Safe Primes Key Generation: (A5112) Safe Primes Key Generation: 2048, 3072, 4096
Key pair verification	DigSig-SigVer	Key pair Verification		ECDSA SigVer (FIPS186-4): (A5112) ECDSA SigVer (FIPS186-5): (A5112) RSA SigVer (FIPS186-4): (A5112) RSA SigVer (FIPS186-5): (A5112) Safe Primes Key Verification: (A5112)
KAS	KAS-Full	Key Agreement	IG:IG D.F Scenario 2, path (2) Key confirmation:no Key derivation:IG 2.4.B SP 800- 135rev1 CVL Caveat:EC Diffie-Hellman	KAS-ECC-SSC Sp800-56Ar3: (A5112) curve: P-384 Encryption strength: 192 bits KAS-FFC-SSC Sp800-56Ar3: (A5112) [L, N]: [2048,

Name	Type	Description	Properties	Algorithms
			shared secret computation provides between 112 and 256 bits of encryption strength.	256] or [3072, 256] Encryption strength: 112 or 128 bits

Table 8: Security Function Implementations

2.7 Algorithm Specific Information

AES-GCM IV Generation

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

Firmware AES-GCM

The module's IPsec firmware AES-GCM implementation conforms to IG C.H, scenario #1. IV generation of IPsec AES-GCM implementation is compliant with RFC 4106 and the IKEv2 protocol RFC 7296 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 values for a given session key, the first party, client, or server, which encounters this condition will trigger a handshake to establish a new encryption key. The IPsec AES-GCM IV is only used in context of the AES GCM mode encryption within the IPsec protocol. In cases where the module 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 C.H, 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 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 used in the context of the AES GCM mode encryption within the TLS protocol. In cases where the module power is lost and then restored, the key used for TLS 1.2 AES-GCM shall be regenerated.

The module's TLS 1.3 firmware AES-GCM implementation conforms to IG C.H Scenario #5 and RFC 8446. The module supports acceptable AES-GCM cipher suites for TLS 1.3 from section 3.3.1.2 of SP800-52 revision 2 and confirms that the IV is generated and used within the protocol's implementation. The counter portion of the IV is set by the module within its cryptographic boundary. In cases where the module power is lost and then restored, the key used for TLS 1.3 AES-GCM shall be regenerated.

The module's SSHv2 firmware AES-GCM implementation conforms to IG C.H, 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 used in the context of the AES GCM mode encryption within the SSHv2 protocol. In cases where the module power is lost and then restored, the key used for SSHv2 AES-GCM shall be regenerated.

Hardware AES-GMAC and AES-GCM

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 C.H, 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 of NIST SP 800-38D, the probability that the authenticated encryption function will ever 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 cases where the module power is lost and then restored, the keys used for AES-GCM shall be regenerated.

2.8 RNG and Entropy

Cert Number	Vendor Name
E182	Infinera Corporation

Table 9: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Infinera Groove CPU Time Jitter RNG Entropy Source	Non-Physical	Yocto Linux Kernel 5.10 on NXP QorIQ® P-2040 Processors	64 bits	0.33 bits	SHA3-256

Table 10: Entropy Sources

The module offers an SP800-90Arev1-compliant Deterministic Random Bit Generator (DRBG) utilizing the CTR_DRBG mechanism with AES-256 for generating key components of asymmetric keys and random numbers. The entropy source, as detailed in the tables within this section, resides within the module's cryptographic boundary. The entropy source provides an output of 256 bits with full entropy.

2.9 Key Generation

To generate RSA, ECDSA and EC Diffie-Hellman keys, the module implements asymmetric key generation services compliant with FIPS186-5 and using a DRBG compliant with SP800-90Arev1.

The random values used in asymmetric key generation are obtained from the DRBG. In accordance with FIPS 140-3 IG D.H, the cryptographic module performs Cryptographic Key Generation (CKG) for asymmetric keys as per section 5.1 of SP800-133rev2 (vendor affirmed) by obtaining a random bit string directly from an approved DRBG and that can support the required security strength requested by the caller ("V" is always equal to 0, i.e., B=U, as described in Additional Comments 2 of IG D.H).

The module does not provide a dedicated service for generating symmetric keys. However, symmetric keys can be derived using SP800-135rev1 for TLS KDF algorithm. This generation method maps to section 6.2.1 of SP800-133rev2.

2.10 Key Establishment

The module provides EC Diffie-Hellman shared secret computation compliant with SP800-56Arev3, in accordance with scenario 2 (1) of IG D.F.

The module provides SP800-38F approved key transport methods according to IG D.G. The key transport method is provided using an AES-KW key wrapping algorithm.

According to “Table 2: Comparable strengths” in SP800-57, the key sizes of AES and EC Diffie-Hellman provide the following security strengths:

- EC Diffie-Hellman shared secret computation provides between 112 and 256 bits of encryption strength.
- AES key wrapping provides between 128 and 256 bits of encryption strength.

Additionally, the module also supports key derivation using TLS 1.2 KDF compliant with SP800-135rev1.

2.11 Industry Protocols

The module supports SSHv2, TLS v1.2, TLSv1.3, SNMPv3 and IPsec/IKEv2 industrial protocols. Please refer to SSPs Table for more information.

3 Cryptographic module interfaces

3.1 Ports and Interfaces

The module provides a few 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)

Physical Port	Logical Interface(s)	Data That Passes
PWR Input	Power	N/A.
PWR RTN	Power	N/A.
CFP2-ACO	Data Input Data Output Control Input Status Output	Customer traffic data input. Customer traffic data output. Northbound control messages input. Alarms, status, operational results output.

Physical Port	Logical Interface(s)	Data That Passes
CFP2-DCO	Data Input Data Output Control Input Status Output	Customer traffic data input. Customer traffic data output. Northbound control messages input. Alarms, status, operational results output.
LC	Data Input Data Output Control Input Status Output	Customer traffic data input. Customer traffic data output. Northbound control messages input. Alarms, status, operational results output.
MTP	Data Input Data Output Control Input Status Output	Customer traffic data input. Customer traffic data output. Northbound control messages input. Alarms, status, operational results output.
OFP2	Data Input Data Output Control Input Status Output	Customer traffic data input. Customer traffic data output. Northbound control messages input. Alarms, status, operational results output.
QSFP+	Data Input Data Output Control Input Status Output	Customer traffic data input. Customer traffic data output. Northbound control messages input. Alarms, status, operational results output.
QSFP28	Data Input Data Output Control Input Status Output	Customer traffic data input. Customer traffic data output. Northbound control messages input. Alarms, status, operational results output.
SFP+	Data Input Data Output Control Input Status Output	Customer traffic data input. Customer traffic data output. Northbound control messages input. Alarms, status, operational results output.
SFP	Data Input Data Output Control Input Status Output	Customer traffic data input. Customer traffic data output. Northbound control messages input. Alarms, status, operational results output.

Physical Port	Logical Interface(s)	Data That Passes
Type-C	Data Input Data Output Control Input Status Output	Customer traffic data input. Customer traffic data output. Northbound control messages input. Alarms, status, operational results output.
RJ45	Control Input Status Output	Northbound control messages input. Alarms, status, operational results output.
RS232	Control Input Status Output	Northbound control messages input. Alarms, status, operational results output.
Pull Button	Control Input	Card pulled-out message input.
Reset Button	Control Input	Module reset message input.
LED	Status Output	Status output.

Table 11: Ports and Interfaces

Note: Some of the ports on the line cards contain in-band channels (OSC, GCC) for module management purposes. Therefore, "Control Input Interface" and "Status Output Interface" are listed under these ports.

4 Roles, services, and authentication

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
Password	The minimum length is eight (8) to 128 possible characters. The configuration supports at most ten failed attempts to authenticate in a one minute period.	ID & Password combination used within a challenge/response mechanism	The probability that a random attempt will succeed or a false acceptance will occur is $1/(94^8)$ which is less than 1/1,000,000.	Maximum nine (9) consecutive and invalid attempts. The probability of successfully authenticating to the module within one minute is $9/(94^8)$, which is less than 1/100,000.
Public key	User/CO authentication via SSH.	RSA 2048 / ECDSA P-224	Strength of signature algorithm, minimum 112-bits. Probability	Maximum nine (9) consecutive and invalid attempts. The probability of successfully

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
			of success for random attempt: $1/(2^{112})$ which is less than 1/1,000,000.	authenticating to the module within one minute is $9/(2^{112})$, which is less than 1/100,000.

Table 12: Authentication Methods

4.1.1 Password-based authentication

The operators must be authenticated by the cryptographic module before accessing services that require the assumption of an authorized role. The module authenticates operators using their usernames and passwords. 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 can enter to execute its services.

The following rules apply to password complexity:

- The password length must be between 8 and 128 characters.
- At least one character from each of the following sets must be present:
 - Numeric characters
 - Lower-case alphabetical characters
 - Upper-case alphabetical characters
 - Special characters (~!@#\$%^&* _-+=`|()\{}[]:;<>,.? ' / ")
- The previous five passwords must not be used.
- The password must not include more than two consecutive repetitions of the same character.
- UID must not be contained in the 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 lower-case alphabetic characters, 26 upper-case alphabetical characters, and 32 special characters to choose from in total. The calculation should be $10 \times 9 \times 9 \times 9 \times 9 \times 26 \times 26 \times 32 = 1,419,275,520$).

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.

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-SECURITY`), when the maximum number of consecutive and invalid attempts (maximum is 9) is reached. Therefore, the associated probability of a successful random attempt during a one-minute period is less than $9/1,419,275,520 = 6.34126 \times 10^{-9}$, 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 form the password.

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

4.1.2 Public key based SSH authentication

Besides the password-based authentication, the authentication based on the public key is also supported by the module when users log in to the module with secure shell (SSH).

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 bits. The chance of a random authentication attempt falsely succeeding is: $1/2^{112}$ which is less than $1/1,000,000$, 1.92×10^{-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 $9/2^{112}$, 1.73×10^{-33} , which is also much less than one in 100,000.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
crypto-officer	Identity	CO	Password Public key
administration	Identity	CO	Password Public key
configuration	Identity	User	Password Public key
operation	Identity	User	Password Public key
supervision	Identity	User	Password Public key

Table 13: 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 retrieval, etc. Detailed services provided for them are listed in the table in section [4.3 Approved Services](#).

The module has five user group levels, which are mapped to the CO role and User role as listed in the table below. Users in crypto-officer and administration groups are CO role users. Crypto-officer users can execute all the operations of the module, while administration users can execute all operations except those associated with data path encryption (ODU encryption). Users in configuration, operation and supervision groups are User role users.

Multiple concurrent users can access a single module simultaneously. Identification and authorization are facilitated through a username and an authentication method. The user group is determined during user creation, and there is no operation available to modify the user group afterward.

The module does not support a maintenance role.

4.3 Approved Services

Services of the authorized CO and User roles are listed in the table below.

The following indicators are used to show the type of access required for the SSP:

R – Read. The SSP is read.

W – Write. The SSP is established, generated, modified, or zeroized.

E – Execute. The SSP is used within an approved or allowed security function or authentication mechanism.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Module initialization	Initialize the module	A system restart "complete" response after the initialization command is issued	Command	Status output	RNG	crypto-officer - Master key: W - Seed to DRBG: R - DRBG V: G - DRBG key: G
Network Element Information	Configure and show Network Element Information	A "complete" response to the command	Command and parameters	Command response	None	crypto-officer administration configuration operation supervision
FIPS mode setting	Switch from FIPS-approved security function mode to FIPS non-approved security function mode	A "complete" response to the command	Command and parameters	Command response	None	crypto-officer - Master key: Z
FIPS mode displaying	Show current mode of operation	A "complete" response to the command	Command and parameters	Command response	None	crypto-officer administration configuration operation supervision
Management of	Generate asymmetric key pairs for	A "complete"	Command and	Command	Key pair generation	crypto-officer - SSHv2

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
asymmetric key pairs	certificate and SSH	response to the command	parameters	response		server private key - ECDSA: W - SSHv2 server public key - ECDSA: W - SSHv2 server private key - RSA: W - SSHv2 server public key - RSA: W
Management of certificates	Generate CSR, Export CSR, Import signed CA certificate, Import root CA certificate.	A "complete" response to the command	Command and parameters	Command response	Key pair generation	crypto-officer - CSR for TLS and IPsec - RSA: R,E - CSR for TLS and IPsec - ECDSA: R,E - CA certificate for TLS and IPsec - RSA: R,E - CA certificate for TLS and IPsec - ECDSA: R,E - NE local certificate for TLS and IPsec - ECDSA: R,E - NE local certificate for TLS and IPsec - RSA: R,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Datapath encryption	Encrypt user data, and manage the data path encryption key	A "complete" response to the command	Command and parameters	Command response	Authenticated Encryption	crypto-officer - ODU encryption AES-GMAC key: E - ODU encryption AES-GCM key: E
Datapath decryption	Decrypt user data, and manage the data path decryption key	A "complete" response to the command	Command and parameters	Command response	Authenticated Decryption	crypto-officer - ODU encryption AES-CTR key: E - ODU encryption AES-GMAC key: E
Management of TLS session for datapath encryption key-Sync	Establish TLS session for datapath encryption key-Sync	A "complete" response to the command	Command and parameters	Command response	Authenticated Decryption Authenticated Encryption Message Authentication Key pair generation Key pair verification	crypto-officer - TLS(DHE-RSA) session key: G,E - Elliptic Curve Diffie-Hellman private key: G,E - Elliptic Curve Diffie-Hellman public key: G,E - Elliptic Curve Diffie-Hellman shared secret: G,E - Diffie-Hellman private key: G,E - Diffie-Hellman public key: G,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Diffie-Hellman shared secret: G,E - TLS (DHE-RSA) preMaster secret: G,E - TLS(DHE-RSA) Master Secret: G,E - TLS(ECDH E-ECDSA) preMaster secret: G,E - TLS(ECDH E-ECDSA) Master Secret: G,E - TLS(ECDH E-ECDSA) session key: G,E - TLS HMAC: G,E
Monitor alarms	Monitor alarms for diagnostic purposes	Alarms output	Command	Status output	None	crypto-officer administration configuration operation supervision
View system logs	View system status messages in historical alarm logs and provisioning logs	System logs output	Command	Status output	None	crypto-officer administration configuration operation supervision
Device diagnostics	Test the module during operation	A "complete"	Command and	Command respons	None	crypto-officer administrati

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		response to the command	parameters	and status via logs and LEDs		on configuration operation supervision
IPsec	Secure, rekeying, and communications between the module and the management system over DCN	A "complete" response to the command	Command and parameters	Command response and Status output	Authenticated Decryption Authenticated Encryption Message Authentication Key pair generation Key pair verification	crypto-officer - CA certificate for TLS and IPsec - RSA: E - CA certificate for TLS and IPsec - ECDSA: E - ESP AES: E - IPsec Pre Shared Secret: E - System private Key for TLS and IPsec - RSA: E - System public Key for TLS and IPsec - RSA: E - System private Key for TLS and IPsec - ECDSA: E - System public Key for TLS and IPsec - ECDSA: E - CSR for TLS and IPsec - ECDSA: E - NE local certificate for TLS and

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						IPsec - ECDSA: E - CSR for TLS and IPsec - RSA: E - NE local certificate for TLS and IPsec - RSA: E - IKEv2 HMAC: G,E - ESP HMAC: G,E - IKEv2 AES: E
Zeroization	Zeroize the CSPs and SSPs	A "complete " response to the command	Comman d	Comma nd respons e	None	crypto- officer - Master key: Z
on demand self-tests	Perform self- tests on demand	A system restart "complete " output after self- test	Comman d	Status output	None	crypto- officer administrati on configuratio n operation supervision
L1 data path Service	Perform L1 data path service provisioning and status retrieval.	A "complete " response to the command	Comman d	Comma nd respons e	None	crypto- officer administrati on configuratio n operation supervision
L0 optical service	Perform L0 optical related service provisioning and status retrieval.	A "complete " response to the command	Comman d	Comma nd respons e	None	crypto- officer administrati on configuratio n operation supervision

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
L1 OTN service	Perform L1 OTN related service provisioning and status retrieval.	A "complete" response to the command	Command	Command response	None	crypto-officer administration configuration operation supervision
CLI	Access the module through Secure Shell (SSH)	A "complete" response to the command	Command	Command response	Authenticated Decryption Authenticated Encryption Decryption Encryption Message Authentication Key pair generation Key pair verification	crypto-officer - SSH session Key: R - SSH authentication key: R - PID: W,E administration - SSH session Key: R - SSH authentication key: R - PID: W,E configuration - SSH session Key: R - SSH authentication key: R - PID: W,E operation - SSH session Key: R - SSH authentication key: R - PID: W,E supervision - SSH session Key: R - SSH authentication

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						on key: R - PID: W,E
CLI commands set	Upload and execute CLI commands set	A "complete" response to the command	Command	Command response	Authenticated Decryption Authenticated Encryption Message Authentication Key pair generation Key pair verification	crypto-officer - SSH session Key: R - SSH authentication on key: R administration - SSH session Key: R - SSH authentication on key: R configuration - SSH session Key: R - SSH authentication on key: R operation - SSH session Key: R - SSH authentication on key: R supervision - SSH session Key: R - SSH authentication on key: R
Key Wrap	Wrap the key for ODU encryption during synchronization with peer	A "complete" response to the command	None	Command response	KTS-KeyWrap	crypto-officer - Key Wrap Key: R
SNMPv3	SNMPv3 service	A "complete	Command	Command	Decryption Encryption	crypto-officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		" response to the command		response	Message Authenticati on	- SNMPv3 Privacy Passphrase: R - SNMPv3 Authenticati on Passphrase: R - SNMPv3 Privacy key: R - SNMPv3 Authenticati on key: R administrati on - SNMPv3 Privacy Passphrase: R - SNMPv3 Authenticati on Passphrase: R - SNMPv3 Privacy key: R - SNMPv3 Authenticati on key: R configuratio n - SNMPv3 Privacy Passphrase: R - SNMPv3 Authenticati on Passphrase: R - SNMPv3 Privacy key: R - SNMPv3 Authenticati on key: R

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						operation - SNMPv3 Privacy Passphrase: R - SNMPv3 Authentication Passphrase: R - SNMPv3 Privacy key: R - SNMPv3 Authentication key: R supervision - SNMPv3 Privacy Passphrase: R - SNMPv3 Authentication Passphrase: R - SNMPv3 Privacy key: R - SNMPv3 Authentication key: R
RADIUS over IPsec	Remote User authentication	A "complete" response to the command	Command	Command response	None	crypto-officer - IPsec Pre Shared Secret: R,E administration - IPsec Pre Shared Secret: R,E configuration - IPsec Pre Shared Secret: R,E operation - IPsec Pre

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Shared Secret: R,E supervision - IPsec Pre Shared Secret: R,E
TACACS+ over IPsec	Remote User authentication	A "complete" response to the command	Command	Command response	None	crypto-officer - IPsec Pre Shared Secret: R,E administration - IPsec Pre Shared Secret: R,E configuration - IPsec Pre Shared Secret: R,E operation - IPsec Pre Shared Secret: R,E supervision - IPsec Pre Shared Secret: R,E
Telemetry	Status subscription	A "complete" response to the command	Command	Command response	Authenticated Decryption Authenticated Encryption Message Authentication Key pair generation Key pair verification	crypto-officer - CA certificate for TLS and IPsec - RSA: R,E - CA certificate for TLS and IPsec - ECDSA: R,E administration - CA certificate for TLS and IPsec - RSA: R,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- CA certificate for TLS and IPsec - ECDSA: R,E configuration - CA certificate for TLS and IPsec - RSA: R,E - CA certificate for TLS and IPsec - ECDSA: R,E operation - CA certificate for TLS and IPsec - RSA: R,E - CA certificate for TLS and IPsec - ECDSA: R,E supervision - CA certificate for TLS and IPsec - RSA: R,E - CA certificate for TLS and IPsec - ECDSA: R,E
WebGUI	Access the module through HTTPS	A login interface in the web browser	Command	Command response	Authenticated Decryption Authenticated Encryption Message	crypto-officer - CA certificate for TLS and IPsec -

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					Authentication Key pair generation Key pair verification	RSA: R,E - CA certificate for TLS and IPsec - ECDSA: R,E administrati on - CA certificate for TLS and IPsec - RSA: R,E - CA certificate for TLS and IPsec - ECDSA: R,E configuratio n - CA certificate for TLS and IPsec - RSA: R,E - CA certificate for TLS and IPsec - ECDSA: R,E operation - CA certificate for TLS and IPsec - RSA: R,E - CA certificate for TLS and IPsec - ECDSA: R,E supervision - CA certificate for TLS and

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						IPsec - RSA: R,E - CA certificate for TLS and IPsec - ECDSA: R,E
RestConf	Access the module through HTTPS	A "complete" response to the command	Command	Command response	Authenticated Decryption	crypto-officer - CA certificate for TLS and IPsec - RSA: R,E - CA certificate for TLS and IPsec - ECDSA: R,E administration - CA certificate for TLS and IPsec - RSA: R,E - CA certificate for TLS and IPsec - ECDSA: R,E configuration - CA certificate for TLS and IPsec - RSA: R,E - CA certificate for TLS and IPsec - ECDSA: R,E operation - CA

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						certificate for TLS and IPsec - RSA: R,E - CA certificate for TLS and IPsec - ECDSA: R,E supervision - CA certificate for TLS and IPsec - RSA: R,E - CA certificate for TLS and IPsec - ECDSA: R,E
NetConf	Access the module through SSH	A "complete" response to the command	Command	Command response	Authenticated Decryption Authenticated Encryption Message Authentication Key pair generation Key pair verification	crypto-officer - SSH session Key: R,E - SSH authentication on key: R,E administration - SSH session Key: R,E - SSH authentication on key: R,E configuration - SSH session Key: R,E - SSH authentication on key: R,E operation - SSH session

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key: R,E - SSH authentication key: R,E supervision - SSH session Key: R,E - SSH authentication key: R,E
File Service	Access files through SSH	A "complete" response to the command	Command	Command response	Authenticated Decryption Authenticated Encryption Message Authentication Key pair generation Key pair verification	crypto-officer - SSH session Key: R,E - SSH authentication key: R,E administration - SSH session Key: R,E - SSH authentication key: R,E configuration - SSH session Key: R,E - SSH authentication key: R,E operation - SSH session Key: R,E - SSH authentication key: R,E supervision - SSH session Key: R,E - SSH authentication key: R,E

Table 14: Approved Services

4.4 Non-Approved Services

Name	Description	Algorithms	Role
Message Digest	Message Digest used in RADIUS and SNMPv3 protocols	MD5	crypto-officer; administration; configuration; operation; supervision
Decryption	SNMPv3 privacy decryption	DES	crypto-officer; administration; configuration; operation; supervision
Encryption	SNMPv3 privacy encryption	DES	crypto-officer; administration; configuration; operation; supervision

Table 15: Non-Approved Services

4.5 External Software/Firmware Loaded

The module supports the firmware load test by using RSA 2048 with SHA2-256 for the new validated firmware to be uploaded into the module. A Firmware Load Test Key was preloaded to the module's binary at the factory and used for firmware load test. In order to load new firmware, the Crypto Officer must authenticate to the module before loading the firmware. This ensures that unauthorized access and use of the module is not performed. The module will load the new update upon reboot. The update attempt will be rejected if the verification fails.

Firmware loaded into the cryptographic module that is not on the FIPS 140-3 certificate is out of the scope of this validation and requires a separate FIPS 140-3 validation.

5 Software/Firmware security

5.1 Integrity Techniques

The integrity of the module is verified by comparing CRC32 values calculated at the run time on the image file, with the CRC32 values stored in the module's SD card that were computed at the build time.

5.2 Initiate on Demand

The module provides on-demand integrity tests. The on-demand integrity test is performed by power-cycling.

6 Operational environment

Type of Operational Environment: Limited

The module operates in a limited operating environment.

Each Infinera Groove G30 Cryptographic Module has control over its own SSPs.

The CSP access right and Public Security Parameters (PSP) modification right are controlled by the user role authentication. Unauthorized access to the CSPs and SSPs on the module is prohibited no matter if the CSPs and SSPs are on the SD card or the RAM. This ensures that direct access to CSPs and SSPs is restricted to the cryptographic module and the trusted parts of the operational environment.

Processes running on the cryptographic module are owned by the module itself and are not owned by external processes or operators.

7 Physical security

The module is a multi-chip standalone cryptographic module which offers the following physical security mechanisms:

- Production-grade components and production-grade opaque enclosure. The module is completely enclosed in a rectangular hot dip galvanized steel and cold rolled steel with clear zinc plated enclosure.
- Service cards are installed in slots on the shelf.
- All unpopulated slots are equipped with filler cards.

The module does not implement a maintenance role and has no maintenance access interface.

8 Non-invasive security

N/A for this module.

9 Sensitive security parameters management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
EEPROM	Non-volatile memory (Electrically Erasable Programmable Read Only Memory) used to store master key and make it persistent to a reset or a power-off/power-on sequence of the security module.	Static
RAM	Volatile memory used to store SSPs between two consecutive resets or power-on/power-off sequence of the security module. ODU encryption keys are stored in SRAM. All the CSPs and SSPs invoked by the firmware are stored in DRAM.	Dynamic
SD card	Non-volatile memory (Nand flash-based) used to store SSPs and make them persistent to a reset or a power-off/power-on sequence of the security module. All the CSPs and PSPs other than the master key are stored on the SD card.	Static

Table 16: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Input plaintext	External entities	module	Plaintext	Automated	Electronic	
Key Wrapping for datapath encryption keys	module	External entities	Encrypted	Automated	Electronic	AES-KW (A5112)
Key Wrapping for configurations	module	External entities	Encrypted	Automated	Electronic	AES-KW (A5112)

Table 17: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
FIPS/NONFIPS mode switching	Zeroize SSPs when the module is changed from non-FIPS to FIPS or vice versa	Changing FIPS mode means SSPs should not be persisted	CO changes the FIPS mode of the mode
Manual	Zeroize SSPs when CO issues a manual zeroization command	Zeroize CSPs stored in RAM, SD card and EEPROM.	CO issues a manual zeroization command
Power cycle	Zeroize SSPs when reboot.	Zeroize CSPs stored in RAM	CO issues reboot command

Table 18: SSP Zeroization Methods

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

Each key input to 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 140-3 standard requirements, all data output interfaces except the status output interface are inhibited during the key entry/output processes.

The module has a master key stored on the EEPROM of the system. The master key is initialized when the module is switched from the FIPS non-approved mode to the FIPS approved mode. The master key is zeroized automatically when the module is switched from the FIPS approved mode to the FIPS non-approved mode or when the Crypto Officer manually zeroizes the keys. The EEPROM of the master key will be reset to 0xFF 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 the FIPS approved mode to the FIPS non-approved mode by the Crypto Officer.

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

9.4 SSPs

- Random number

In the FIPS approved mode of operation, the module uses SP800-90B compliant RNG Entropy (ESV Cert. #E182) 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.

These seed values are temporarily stored in RAM and are zeroized by power cycling the module. These values are not accessible to any users. 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”, “ODU encryption AES-GCM key” and “ODU encryption AES-GMAC key” in the table below can be transported out of the module with the 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.

Some other keys can be transported into the module with approved symmetric encryption mode (AES) together with an approved authentication method (HMAC-SHA2), which is considered an approved key-wrapping technique according to FIPS 140-3 IG Annex D.H.

- 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 9.5 that states “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.F scenario 2 (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.

- Critical security parameters and public security parameters

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

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
IKEv2 HMAC	Session key integrity check	256 bits HMAC-SHA256 ; 384 bits HMAC-SHA384 ; 512 bits HMAC-	Symmetric key - CSP - CSP			Message Authentication

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		SHA512 - 256				
ESP HMAC	Session key Authentication	256 bits HMAC-SHA256 ; 384 bits HMAC-SHA384 ; 512 bits HMAC-SHA512 - 256	Symmetric key - CSP - CSP			Message Authentication
IKEv2 AES	IKEv2 Session key	128 bits, 256 bits - 128, 256	Symmetric key - CSP - CSP	KDF IKEv2 (A5112)		Authenticated Decryption Authenticated Encryption Decryption Encryption
ESP AES	IPsec session key	128 bits, 256 bits - 128, 256	Symmetric key - CSP - CSP	KDF IKEv2 (A5112)		Authenticated Decryption Authenticated Encryption Decryption Encryption
IPsec Pre Shared Secret	IKEv2 authentication	128 bits ~ 256 bits in HEX string - N/A	Shared secret - CSP - CSP	Input by CLI command		KDF IKEv2 (A5112)
Seed to DRBG	Used for functions requiring random numbers	384 bits - 256	Seed - CSP - CSP	Entropy Source		RNG
DRBG V	Internal state value for the DRBG	256 bits, 320 bits, 384 bits - 128, 192, 256	Internal state - CSP - CSP	Counter DRBG (A5112)		RNG

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
DRBG key	Internal state value for the DRBG	256 bits - 256	Internal state - CSP - CSP	Counter DRBG (A5112)		RNG
Master key	Key to encrypt other SSPs	256 bits - 256	Symmetric key - CSP - CSP	Counter DRBG (A5112)		KTS-KeyWrap
PID	User password for user credential	8 ~ 128 bytes string - N/A	Password - CSP - CSP	Input by CLI command		
Elliptic Curve Diffie-Hellman private key	Elliptic Curve Diffie-Hellman private key	p-384 curve: 384 bits; p-521 curve: 521 bits - 192, 256	Private key - CSP - CSP	Key pair generation		Key pair verification TLS v1.2 KDF RFC7627 (A5112) TLS v1.3 KDF (A5112)
Elliptic Curve Diffie-Hellman public key	Elliptic Curve Diffie-Hellman public key	p-384 curve: 384 bits; p-521 curve: 521 bits - 192, 256	Public key - PSP - PSP	CKG		TLS v1.2 KDF RFC7627 (A5112) TLS v1.3 KDF (A5112)
Elliptic Curve Diffie-Hellman shared secret	Elliptic Curve Diffie-Hellman shared secret	p-384 curve: 384 bits; p-521 curve: 521 bits - 192, 256	Private key - CSP - CSP	CKG		TLS v1.2 KDF RFC7627 (A5112) TLS v1.3 KDF (A5112)
Diffie-Hellman private key	Diffie-Hellman private key	2048 bits, 3072 bits - 112, 128	Private key - CSP - CSP	CKG		TLS v1.2 KDF RFC7627 (A5112) TLS v1.3 KDF (A5112)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Diffie-Hellman public key	Diffie-Hellman public key	2048 bits, 3072 bits - 112, 128	Public key - PSP - PSP	CKG		TLS v1.2 KDF RFC7627 (A5112) TLS v1.3 KDF (A5112)
Diffie-Hellman shared secret	Diffie-Hellman shared secret	2048 bits, 3072 bits - 112, 128	Private key - CSP - CSP	CKG		TLS v1.2 KDF RFC7627 (A5112) TLS v1.3 KDF (A5112)
TLS (DHE-RSA) preMaster secret	TLS preMaster secret	2048 bits, 3072 bits - 112, 128	Private key - CSP - CSP			TLS v1.2 KDF RFC7627 (A5112) TLS v1.3 KDF (A5112)
TLS(DHE-RSA) Master Secret	TLS Master Secret	384 bits - 112, 128	Private key - CSP - CSP			TLS v1.2 KDF RFC7627 (A5112) TLS v1.3 KDF (A5112)
TLS(DHE-RSA) session key	TLS session key	128 bits, 256 bits - 128, 256	Symmetric key - CSP - CSP			TLS v1.2 KDF RFC7627 (A5112) TLS v1.3 KDF (A5112)
TLS(ECDHE-ECDSA) preMaster secret	TLS preMaster secret	256 bits, 384 bits, 521 bits - 128, 192, 256	Private key - CSP - CSP			
TLS(ECDHE-ECDSA) Master Secret	TLS Master Secret	384 bits - 128, 192, 256	Private key - CSP - CSP			

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
TLS(ECDHE-ECDSA) session key	TLS session key	128 bits, 256 bits - 128, 256	Symmetric key - CSP - CSP			
System private Key for TLS and IPsec - RSA	System private Key - RSA	2048 bits, 3072 bits - 112, 384	Private key - CSP - CSP	Key pair generation		TLS v1.2 KDF RFC7627 (A5112) TLS v1.3 KDF (A5112)
System public Key for TLS and IPsec - RSA	System public Key - RSA	2048 bits, 3072 bits - 112, 384	Public key - PSP - PSP	Key pair generation		TLS v1.2 KDF RFC7627 (A5112) TLS v1.3 KDF (A5112)
System private Key for TLS and IPsec - ECDSA	System private Key - ECDSA	256 bits; 384 bits; 521 bits - 128, 192, 256	Private key - CSP - CSP	Key pair generation		TLS v1.2 KDF RFC7627 (A5112) TLS v1.3 KDF (A5112)
System public Key for TLS and IPsec - ECDSA	System public Key - ECDSA	256 bits; 384 bits; 521 bits - 128, 192, 256	Public key - PSP - PSP	Key pair generation		TLS v1.2 KDF RFC7627 (A5112) TLS v1.3 KDF (A5112)
TLS HMAC	TLS HMAC	256 bits; 384 bits - 256	Symmetric key - CSP - CSP			Message Authentication
SNMPv3 Privacy Passphrase	SNMPv3 Privacy secret	8 ~ 64 bytes string -	Passphrase - CSP - CSP	Input by CLI command		
SNMPv3 Authentication Passphrase	SNMPv3 Authentication secret (8 ~ 64 bytes string)	8 ~ 64 bytes string -	Passphrase - CSP - CSP	Input by CLI command		

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
SNMPv3 Privacy key	SNMPv3 Privacy Key	128 bits - 128	Symmetric key - CSP - CSP	KDF SNMP (A5112)		
SNMPv3 Authentication key	HMAC key	160 bits - 128	Symmetric key - CSP - CSP	KDF SNMP (A5112)		Message Authentication
ODU encryption AES-CTR key	ODU encryption AES-CTR key	256 bits - 256	Symmetric key - CSP - CSP	Counter DRBG (A5112)		AES-CTR (A5078) AES-CTR (A5112)
ODU encryption AES-GMAC key	ODU encryption AES-GMAC key	256 bits - 256	Symmetric key - CSP - CSP	Counter DRBG (A5112)		AES-GMAC (AES 3844)
ODU encryption AES-GCM key	ODU encryption AES-GCM key	256 bits - 256	Symmetric key - CSP - CSP	Counter DRBG (A5112)		AES-GCM (A5078) AES-GCM (A5112)
Key Wrap Key	Key Wrap Key for ODU encryption keys	256 bits - 256	Symmetric key - CSP - CSP	TLS v1.2 KDF RFC7627 (A5112) TLS v1.3 KDF (A5112)		Decryption Encryption Message Authentication
SSHv2 server private key - ECDSA	SSH Key	256 bits; 384 bits; 521 bits - 128, 192, 256	Private key - CSP - CSP	Key pair generation		Key pair verification ECDSA SigGen (FIPS186-5) (A5112)
SSHv2 server public key - ECDSA	SSH public Key	256 bits; 384 bits; 521 bits - 128, 192, 256	Public key - PSP - PSP	Key pair generation		
SSHv2 server private key - RSA	SSH Key	2048 bits; 3072 bits - 112, 128	Private key - CSP - CSP	Key pair generation		Key pair verification RSA SigGen (FIPS186-5) (A5112)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
SSHv2 server public key - RSA	SSH public Key	2048 bits; 3072 bits - 112, 128	Public key - PSP - PSP	Key pair generation		
SSH session Key	SSH Encryption AES Key	128 bits, 256 bits - 128, 256	Symmetric key - CSP - CSP	KDF SSH (A5112)		Authenticated Decryption Authenticated Encryption Decryption Encryption
SSH authentication key	SSH authentication key used by message authentication function	256 bits, 512 bits - 256	Symmetric key - CSP - CSP	KDF SSH (A5112)		Message Authentication
CSR for TLS and IPsec - ECDSA	CSR (including System public Key) - ECDSA	256 bits; 384 bits; 521 bits - 128, 192, 256	Public key - PSP - PSP	Key pair generation		ECDSA SigGen (FIPS186-5) (A5112)
NE local certificate for TLS and IPsec - ECDSA	NE local certificate (including System public Key) Key - ECDSA	256 bits; 384 bits; 521 bits - 128, 192, 256	Public key - PSP - PSP	Other		ECDSA SigVer (FIPS186-4) (A5112)
CSR for TLS and IPsec - RSA	CSR (including System public Key) - RSA	2048 bits; 3072 bits - 112, 128	Public key - PSP - PSP	Key pair generation		RSA SigGen (FIPS186-5) (A5112)
NE local certificate for TLS and IPsec - RSA	NE local certificate (including System public Key) - RSA	2048 bits; 3072 bits - 112, 128	Public key - PSP - PSP	Installed from the external server		RSA SigVer (FIPS186-5) (A5112)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
CA certificate for TLS and IPsec - RSA	CA certificate - RSA	2048 bits; 3072 bits - 112, 128	Public key - PSP - PSP	installed from the external server		RSA SigVer (FIPS186-4) (A5112) RSA SigVer (FIPS186-5) (A5112)
CA certificate for TLS and IPsec - ECDSA	CA certificate - ECDSA	256 bits; 384 bits; 521 bits - 128, 192, 256	Public key - PSP - PSP	installed from the external server		ECDSA SigVer (FIPS186-5) (A5112)

Table 19: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
IKEv2 HMAC		RAM:Plaintext	Until the IKEv2 session end	Power cycle	
ESP HMAC		RAM:Plaintext	Until the IPsec session end	Power cycle	
IKEv2 AES		RAM:Plaintext	Until the IKEv2 session end	Power cycle	
ESP AES		RAM:Plaintext	Until the IPsec session end	Power cycle	
IPsec Pre Shared Secret	Input plaintext Key Wrapping for configurations	SD card:Encrypted	Until zeroized or replaced by a new one	FIPS/NONFI PS mode switching Manual	
Seed to DRBG		RAM:Plaintext	Until zeroized	FIPS/NONFI PS mode switching Manual Power cycle	DRBG V:Used With DRBG key:Decrypts

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
DRBG V		RAM:Plaintext	Until zeroized	FIPS/NONFI PS mode switching Manual Power cycle	Seed to DRBG:Derived From DRBG key:Decrypts
DRBG key		RAM:Plaintext	Until zeroized	FIPS/NONFI PS mode switching Manual	Seed to DRBG:Encrypts DRBG V:Encrypts
Master key		EEPROM:Plaintext	Until zeroized	FIPS/NONFI PS mode switching Manual	
PID	Input plaintext Key Wrapping for configurations	SD card:Encrypted	Until zeroized or replaced by a new one	FIPS/NONFI PS mode switching Manual	
Elliptic Curve Diffie-Hellman private key		RAM:Plaintext	Until the ECDH session end	FIPS/NONFI PS mode switching Manual Power cycle	Elliptic Curve Diffie-Hellman public key:Paired With Elliptic Curve Diffie-Hellman shared secret:Encrypts
Elliptic Curve Diffie-Hellman public key		RAM:Plaintext	Until the ECDH session end	FIPS/NONFI PS mode switching Manual Power cycle	Elliptic Curve Diffie-Hellman private key:Paired With Diffie-Hellman shared secret:Decrypts
Elliptic Curve Diffie-Hellman shared secret		RAM:Plaintext	Until the ECDH session end	FIPS/NONFI PS mode switching Manual Power cycle	Elliptic Curve Diffie-Hellman private key:Decrypts Elliptic Curve Diffie-Hellman public key:Encrypts
Diffie-Hellman private key		RAM:Plaintext	Until the DH session end	FIPS/NONFI PS mode switching Manual Power cycle	Diffie-Hellman public key:Paired With Diffie-Hellman

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					shared secret:Decrypts
Diffie-Hellman public key		RAM:Plaintext	Until the DH session end	FIPS/NONFI PS mode switching Manual Power cycle	Diffie-Hellman private key:Paired With Diffie-Hellman shared secret:Encrypts
Diffie-Hellman shared secret		RAM:Plaintext	Until the DH session end	FIPS/NONFI PS mode switching Manual Power cycle	Diffie-Hellman private key:Decrypts Diffie-Hellman public key:Encrypts
TLS (DHE-RSA) preMaster secret		RAM:Plaintext	Until the TLS session end	FIPS/NONFI PS mode switching Manual Power cycle	
TLS(DHE-RSA) Master Secret		RAM:Plaintext	Until the TLS session end	FIPS/NONFI PS mode switching Manual Power cycle	TLS (DHE-RSA) preMaster secret:Derived From
TLS(DHE-RSA) session key		RAM:Plaintext	Until the TLS session end	FIPS/NONFI PS mode switching Manual Power cycle	TLS(DHE-RSA) Master Secret:Derived From
TLS(ECDH E-ECDSA) preMaster secret		RAM:Plaintext	Until the TLS session end	FIPS/NONFI PS mode switching Manual Power cycle	
TLS(ECDH E-ECDSA) Master Secret		RAM:Plaintext	Until the TLS session end	FIPS/NONFI PS mode switching Manual Power cycle	TLS(ECDHE-ECDSA) Master Secret:Derived From
TLS(ECDH E-ECDSA) session key		RAM:Plaintext	Until the TLS session end	FIPS/NONFI PS mode switching Manual Power cycle	TLS(ECDHE-ECDSA) Master Secret:Derived From
System private Key for TLS and	Key Wrapping for	SD card:Encrypted	Until zeroized or replaced	FIPS/NONFI PS mode switching Manual	System public Key for TLS and IPsec - RSA:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
IPsec - RSA	configurations		by a new one		
System public Key for TLS and IPsec - RSA	Key Wrapping for configurations	SD card:Encrypted	Until zeroized or replaced by a new one	FIPS/NONFI PS mode switching Manual	System private Key for TLS and IPsec - RSA:Paired With
System private Key for TLS and IPsec - ECDSA	Key Wrapping for configurations	SD card:Encrypted	Until zeroized or replaced by a new one	FIPS/NONFI PS mode switching Manual	System public Key for TLS and IPsec - ECDSA:Paired With NE local certificate for TLS and IPsec - RSA:Used With
System public Key for TLS and IPsec - ECDSA	Key Wrapping for configurations	SD card:Encrypted	Until zeroized or replaced by a new one	FIPS/NONFI PS mode switching Manual	System public Key for TLS and IPsec - ECDSA:Paired With CSR for TLS and IPsec - ECDSA:Used With
TLS HMAC		RAM:Plaintext	Until the TLS session end	FIPS/NONFI PS mode switching Manual Power cycle	
SNMPv3 Privacy Passphrase	Input plaintext Key Wrapping for configurations	SD card:Encrypted	Until zeroized or replaced by a new one	FIPS/NONFI PS mode switching Manual	SNMPv3 Authentication Passphrase:Used With
SNMPv3 Authentication Passphrase	Input plaintext Key Wrapping for configurations	SD card:Encrypted	Until zeroized or replaced by a new one	FIPS/NONFI PS mode switching Manual	SNMPv3 Authentication key:Encrypts
SNMPv3 Privacy key		RAM:Plaintext	Until zeroized or	FIPS/NONFI PS mode switching	SNMPv3 Privacy Passphrase:Encrypts

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
			replaced by a new one	Manual Power cycle	
SNMPv3 Authentication key		RAM:Plaintext	Until zeroized or replaced by a new one	FIPS/NONFI PS mode switching Manual Power cycle	SNMPv3 Privacy key:Derived From
ODU encryption AES-CTR key	Key Wrapping for datapath encryption keys	RAM:Plaintext	Until ODU encryption encryption -interval timeout	FIPS/NONFI PS mode switching Manual Power cycle	
ODU encryption AES-GMAC key	Key Wrapping for datapath encryption keys	RAM:Plaintext	Until ODU encryption encryption -interval timeout	FIPS/NONFI PS mode switching Manual Power cycle	
ODU encryption AES-GCM key		RAM:Plaintext	Until ODU encryption encryption -interval timeout	FIPS/NONFI PS mode switching Manual Power cycle	
Key Wrap Key		RAM:Plaintext	Until zeroized or Keywrapping session end	FIPS/NONFI PS mode switching Manual Power cycle	
SSHv2 server private key - ECDSA		SD card:Encrypted	Until zeroized or replaced by a new one	FIPS/NONFI PS mode switching Manual	SSHv2 server public key - ECDSA:Paired With
SSHv2 server public key - ECDSA		SD card:Encrypted	Until zeroized or replaced by a new one	FIPS/NONFI PS mode switching Manual	SSHv2 server public key - ECDSA:Paired With
SSHv2 server private key - RSA		SD card:Encrypted	Until zeroized or replaced	FIPS/NONFI PS mode switching Manual	SSHv2 server public key - RSA:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
			by a new one		
SSHv2 server public key - RSA		SD card:Encrypted	Until zeroized or replaced by a new one	FIPS/NONFI PS mode switching Manual	SSHv2 server private key - RSA:Paired With
SSH session Key		RAM:Plaintext	Until the SSH session end	FIPS/NONFI PS mode switching Manual	
SSH authentication key		RAM:Plaintext	Until the SSH session end	FIPS/NONFI PS mode switching Manual Power cycle	
CSR for TLS and IPsec - ECDSA		RAM:Plaintext	Until zeroized	FIPS/NONFI PS mode switching Manual Power cycle	System public Key for TLS and IPsec - ECDSA:Encrypts NE local certificate for TLS and IPsec - ECDSA:Used With
NE local certificate for TLS and IPsec - ECDSA		SD card:Encrypted	Until zeroized or replaced by a new one	FIPS/NONFI PS mode switching Manual	CSR for TLS and IPsec - ECDSA:Derived From
CSR for TLS and IPsec - RSA		RAM:Plaintext	Until zeroized	FIPS/NONFI PS mode switching Manual Power cycle	System public Key for TLS and IPsec - RSA:Encrypts NE local certificate for TLS and IPsec - RSA:Used With
NE local certificate for TLS and IPsec - RSA		SD card:Encrypted	Until zeroized or replaced by a new one	FIPS/NONFI PS mode switching Manual	CSR for TLS and IPsec - RSA:Derived From
CA certificate		SD card:Encrypted	Until zeroized	FIPS/NONFI PS mode	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
for TLS and IPsec - RSA			or replaced by a new one	switching Manual	
CA certificate for TLS and IPsec - ECDSA		SD card: Encrypted	Until zeroized or replaced by a new one	FIPS/NONFI PS mode switching Manual	

Table 20: SSP Table 2

9.5 Transitions

In compliance with NIST SP 800-131A Rev. 2, the module supports algorithms and key lengths that provide a minimum of 112 bits of security strength for applying cryptographic protection. Starting January 1, 2031, the minimum security strength for applying cryptographic protection will be 128 bits, and security strengths between 112 bits and 128 bits will be allowed for legacy use only to process information that is already protected.

Please see the latest revision of SP 800-131A and CMVP Programmatic Transitions page for transitions that may affect this module.

10 Self-tests

The module performs both pre-operational 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.

10.1 Pre-operational self-tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
Firmware integrity	CRC-32	EDC	SW/FW Integrity	Firmware starting indicates tests have been run.	FW integrity is verified by computing an EDC (CRC-32) and comparing it to the reference value.

Table 21: Pre-Operational Self-Tests

Each time the cryptographic module is powered up, pre-operational firmware integrity test will be performed. Restarting the cryptographic module provides a means by which the operator can perform pre-operational self-tests on demand.

During pre-operational self-tests, data output is inhibited. Once pre-operational self-tests succeed, data output will resume.

10.2 Conditional self-tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB (A5078)	128 bits, 256 bits	KAT	CAST	Module is in normal state	Symmetric encryption	Test runs at power-on
AES-CBC-Enc	128 bits, 192 bits, 256 bits	KAT	CAST	Module is in normal state	Symmetric Encryption	Test runs at power-on
AES-CBC-Dec	128 bits, 192 bits, 256 bits	KAT	CAST	Module is in normal state	Symmetric Decryption	Test runs at power-on
AES-CTR-Enc	128 bits, 192 bits, 256 bits	KAT	CAST	Module is in normal state	Symmetric Encryption	Test runs at power-on
AES-CTR-Dec	128 bits, 192 bits, 256 bits	KAT	CAST	Module is in normal state	Symmetric Decryption	Test runs at power-on
AES-GCM-Enc	128 bits, 192 bits, 256 bits	KAT	CAST	Module is in normal state	Symmetric Encryption	Test runs at power-on
AES-GCM-Dec	128 bits, 192 bits, 256 bits	KAT	CAST	Module is in normal state	Symmetric Decryption	Test runs at power-on
HMAC-SHA-1 (A5078)	MAC: 96 Key Length: 128-512	KAT	CAST	Module is in normal state	Message authentication	Test runs at power-on
HMAC-SHA2-256 (A5078)	MAC: 128-224 Increment 32 Key Length: 128-512 Increment 192; MAC: 256 Key Length: 128-512 Increment 192; MAC: 384 Key Length: 384-1024 Increment 320; MAC: 512 Key Length: 512-1024 Increment 256	KAT	CAST	Module is in normal state	Message authentication	Test runs at power-on
SHA-1 (A5078)	Message Length: 8-51200	KAT	CAST	Module is in normal state	Message digest	Test runs at power-on

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA2-256 (A5078)	Message Length: 8-51200	KAT	CAST	Module is in normal state	Message digest	Test runs at power-on
SHA3-256 (A5078)	Message Length: 8-65535	KAT	CAST	Module is in normal state	Message digest	Test runs at power-on
RNG SHA3-256	Message Length: 0-65536	KAT	CAST	Module is in normal state	Message digest	Test runs at power-on
AES-ECB (A5112)	128 bits, 256 bits	KAT	CAST	Module is in normal state	Symmetric Encryption, Symmetric Decryption	Test runs at power-on
AES-CBC (A5112)	128 bits, 256 bits	KAT	CAST	Module is in normal state	Symmetric Encryption, Symmetric Decryption	Test runs at power-on
AES-GCM (A5112)	128 bits, 256 bits	KAT	CAST	Module is in normal state	Symmetric Encryption, Symmetric Decryption	Test runs at power-on
AES-KW (A5112)	128 bits, 256 bits	KAT	CAST	Module is in normal state	Symmetric Encryption, Symmetric Decryption	Test runs at power-on
Counter DRBG (A5112)	AES 256; Health test per section 11.3 of SP 800-90Arev1	KAT	CAST	Module is in normal state	Instantiate, generate, reseed, generate (compliant with SP 800-90Ar1)	Test runs at power-on
ECDSA SigGen (FIPS186-5) (A5112)	P-256, P-384, P-521 with SHA2-256, SHA2-384, SHA2-512	KAT	CAST	Module is in normal state	Signature Generation	Test runs at power-on
ECDSA SigVer (FIPS186-5) (A5112)	P-256, P-384, P-521 with SHA1, SHA2-256, SHA2-384, SHA2-512	KAT	CAST	Module is in normal state	Signature Verification	Test runs at power-on
HMAC-SHA-1 (A5112)	MAC: 96-160 Increment 32 Key Length: 128-512 Increment 192	KAT	CAST	Module is in normal state	Message authentication	Test runs at power-on

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA2-224 (A5112)	MAC: 128-224 Increment 32 Key Length: 128-512 Increment 192; MAC: 256 Key Length: 128-512 Increment 192; MAC: 384 Key Length: 384-1024 Increment 320; MAC: 512 Key Length: 512-1024 Increment 256	KAT	CAST	Module is in normal state	Message authentication	Test runs at power-on
KAS-ECC-SSC Sp800-56Ar3 (A5112)	P-384	KAT	CAST	Module is in normal state	Shared secret computation (SP80056Ar3)	Test runs at power-on
KAS-FFC-SSC Sp800-56Ar3 (A5112)	2048 bits	KAT	CAST	Module is in normal state	Shared secret computation (SP80056Ar3)	Test runs at power-on
RSA SigVer (FIPS186-4) (A5112)	2048-bit key with SHA-256	KAT	CAST	Module is in normal state	Signature Verification	Test runs at power-on
RSA SigGen (FIPS186-5) (A5112)	2048-bit key with SHA-256	KAT	CAST	Module is in normal state	Signature Generation	Test runs at power-on
SHA-1 (A5112)	Message Length: 8-51200	KAT	CAST	Module is in normal state	Message digest	Test runs at power-on
SHA2-224 (A5112)	Message Length: 8-51200	KAT	CAST	Module is in normal state	Message digest	Test runs at power-on
KDF SNMP (A5112)	Password Length: 64, 96	KAT	CAST	Module is in normal state	Key derivation	Test runs at power-on
KDF SSH (A5112)	Cipher: AES-128, AES-192, AES-256 Hash Algorithm: SHA-1, SHA2-	KAT	CAST	Module is in normal state	Key derivation	Test runs at power-on

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
	224, SHA2-256, SHA2-384, SHA2-512					
TLS v1.2 KDF RFC7627 (A5112)	Hash Algorithm: SHA2-256, SHA2-384 Key Block Length: 1024	KAT	CAST	Module is in normal state	Key derivation	Test runs at power-on
TLS v1.3 KDF (A5112)	MAC Algorithm: SHA2-256, SHA2-384 KDF Running Modes: DHE, PSK-DHE	KAT	CAST	Module is in normal state	Key derivation	Test runs at power-on
KDF IKEv2 (A5112)	SHA-1, SHA2-256, SHA2-384	KAT	CAST	Module is in normal state	Key derivation	Test runs at power-on
ECDSA KeyGen (FIPS186-5) (A5112)	PCT performed using the generated key pair	PCT	PCT	Module is in normal state	Key generation	key pair generation
RSA KeyGen (FIPS186-5) (A5112)	PCT performed using the generated key pair	PCT	PCT	Module is in normal state	Key generation	key pair generation
Firmware load integrity test with RSA signature	2048 bits	KAT	CAST	Module is in normal state	Key Verification	Firmware with a separate FIPS 140-3 certificate is loaded.
SP800-90B compliant health tests: RCT	1024 samples	RCT	CAST	Module is in normal state	RNG continuous health tests	Test runs at power-on
SP800-90B compliant health tests: APT	1024 samples	APT	CAST	Module is in normal state	RNG continuous health tests	Test runs at power-on
Safe Primes Key Generation (A5112)	ffdhe2048, ffdhe3072, ffdhe4096, modp-2048, modp-3072, modp-4096	KAT	CAST	Module is in normal state	Key Generation	key pair generation

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
Safe Primes Key Verification (A5112)	ffdhe2048, ffdhe3072, ffdhe4096, modp-2048, modp-3072, modp-4096	KAT	CAST	Module is in normal state	Key Verification	key pair generation
AES-CTR (AES 3844)	256 bits	KAT	CAST	Module is in normal state	Symmetric Encryption, Symmetric Decryption	Test runs at power-on
AES-ECB (AES 4707)	256 bits	KAT	CAST	Module is in normal state	Symmetric Encryption, Symmetric Decryption	Test runs at power-on
AES-GCM (AES 4770)	256 bits	KAT	CAST	Module is in normal state	Symmetric Encryption, Symmetric Decryption	Test runs at power-on
AES-GCM (C646)	256 bits	KAT	CAST	Module is in normal state	Symmetric Encryption, Symmetric Decryption	Test runs at power-on
AES-CTR (A5112)	128 bits, 192 bits, 256 bits	KAT	CAST	Module is in normal state	Symmetric Encryption, Symmetric Decryption	Test runs at power-on

Table 22: Conditional Self-Tests

The conditional cryptographic algorithm self-test will be performed prior to the first operational use of the cryptographic algorithm.

Restarting the cryptographic module provides a means by which the operator can perform conditional algorithm self-tests on demand.

The following conditional self-tests are performed while the conditions specified for the following tests are met:

- RSA and ECDSA Pair-wise consistency test
 - RSA Pair-Wise Consistency Test
 - ECDSA Pair-Wise Consistency Test
- 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 140-3 validation.
- SP 800-90B compliant health tests: RCT and APT
- SP 800-90Ar1 DRBG Section 11.3 health test

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

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Firmware integrity	EDC	SW/FW Integrity	On demand	Module reboot

Table 23: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-ECB (A5078)	KAT	CAST	On demand	Module reboot
AES-CBC-Enc	KAT	CAST	On demand	Module reboot
AES-CBC-Dec	KAT	CAST	On demand	Module reboot
AES-CTR-Enc	KAT	CAST	On demand	Module reboot
AES-CTR-Dec	KAT	CAST	On demand	Module reboot
AES-GCM-Enc	KAT	CAST	On demand	Module reboot
AES-GCM-Dec	KAT	CAST	On demand	Module reboot
HMAC-SHA-1 (A5078)	KAT	CAST	On demand	Module reboot
HMAC-SHA2-256 (A5078)	KAT	CAST	On demand	Module reboot
SHA-1 (A5078)	KAT	CAST	On demand	Module reboot
SHA2-256 (A5078)	KAT	CAST	On demand	Module reboot
SHA3-256 (A5078)	KAT	CAST	On demand	Module reboot
RNG SHA3-256	KAT	CAST	On demand	Module reboot
AES-ECB (A5112)	KAT	CAST	On demand	Module reboot
AES-CBC (A5112)	KAT	CAST	On demand	Module reboot
AES-GCM (A5112)	KAT	CAST	On demand	Module reboot
AES-KW (A5112)	KAT	CAST	On demand	Module reboot
Counter DRBG (A5112)	KAT	CAST	On demand	Module reboot
ECDSA SigGen (FIPS186-5) (A5112)	KAT	CAST	On demand	Module reboot
ECDSA SigVer (FIPS186-5) (A5112)	KAT	CAST	On demand	Module reboot
HMAC-SHA-1 (A5112)	KAT	CAST	On demand	Module reboot

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-224 (A5112)	KAT	CAST	On demand	Module reboot
KAS-ECC-SSC Sp800-56Ar3 (A5112)	KAT	CAST	On demand	Module reboot
KAS-FFC-SSC Sp800-56Ar3 (A5112)	KAT	CAST	On demand	Module reboot
RSA SigVer (FIPS186-4) (A5112)	KAT	CAST	On demand	Module reboot
RSA SigGen (FIPS186-5) (A5112)	KAT	CAST	On demand	Module reboot
SHA-1 (A5112)	KAT	CAST	On demand	Module reboot
SHA2-224 (A5112)	KAT	CAST	On demand	Module reboot
KDF SNMP (A5112)	KAT	CAST	On demand	Module reboot
KDF SSH (A5112)	KAT	CAST	On demand	Module reboot
TLS v1.2 KDF RFC7627 (A5112)	KAT	CAST	On demand	Module reboot
TLS v1.3 KDF (A5112)	KAT	CAST	On demand	Module reboot
KDF IKEv2 (A5112)	KAT	CAST	On demand	Module reboot
ECDSA KeyGen (FIPS186-5) (A5112)	PCT	PCT	On demand	Module reboot
RSA KeyGen (FIPS186-5) (A5112)	PCT	PCT	On demand	Module reboot
Firmware load integrity test with RSA signature	KAT	CAST	On demand	Module reboot
SP800-90B compliant health tests: RCT	RCT	CAST	On demand	Module reboot
SP800-90B compliant health tests: APT	APT	CAST	On demand	Module reboot
Safe Primes Key Generation (A5112)	KAT	CAST	On demand	Module reboot

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Safe Primes Key Verification (A5112)	KAT	CAST	On demand	Module reboot
AES-CTR (AES 3844)	KAT	CAST	On demand	Module reboot
AES-ECB (AES 4707)	KAT	CAST	On demand	Module reboot
AES-GCM (AES 4770)	KAT	CAST	On demand	Module reboot
AES-GCM (C646)	KAT	CAST	On demand	Module reboot
AES-CTR (A5112)	KAT	CAST	On demand	Module reboot

Table 24: Conditional Periodic Information

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Error State	Module has failed a Self-Test. FIPS approved services are not provided by the module when it is in this state and data output is inhibited.	Self-Tests Failure	Power Cycle	System Halt

Table 25: Error States

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.

In cases of the error state, the module must be powered-off to clear the error condition. When power-on is executed again, self-tests are also executed like an on-demand operator reset. If the module continuously enters the error state despite multiple trials of reboot, it should be returned to the factory for recovery.

11 Life-cycle assurance

11.1 Installation, Initialization, and Startup Procedures

The Crypto Officer must follow *Groove G30 DCI Quick Installation Guides* and *Groove G30 Commissioning Guide* to have the initial setup. Authorized customers can download the documents from Infinera technical support website <https://infinera.lightning.force.com/lightning/n/Downloads2>.

“Basic Commissioning” described in this section is the operation to install a firmware load on the new Infinera Groove G30 Cryptographic Module.

Basic Commissioning preconditions

- 1) A serial cable (RS232 compliant) connecting from Infinera Groove G30 Cryptographic Module to the serial terminal.
- 2) A CAT5 Ethernet cable connecting from Infinera Groove G30 Cryptographic Module LCI interface to the customer's network.
- 3) A customer's FTP server with FP4.6.6 firmware image available for download.

Basic Commissioning procedures

- 1) Power up the module and then type `uboot` in the console terminal to halt the auto-boot process. Ensure that the serial interface baud-rate remains at the default setting of 9600.
- 2) When prompted in the uboot window, type `run bcmode` to initiate a system reset, returning you to a Linux prompt.
 - a) If the chassis type is GQS-G30CHASF-00, execute the following command:

```
/sbin/mkfs.ext4 /dev/sda1
```

Otherwise, execute:

```
/sbin/mkfs.ext4 /dev/mmcblk0p1
```
 - b) Execute the following commands:

```
mkdir /mnt/flashdisk  
mount -t jffs2 -o ro,noatime /dev/mtdblock1 /mnt/flashdisk  
/mnt/flashdisk/init_sys
```
 - c) After the system restarts, type `uboot` and enter `run bcmode` in the prompted uboot window again.
- 3) In BC mode, execute the following commands:

```
mkdir /mnt/flashdisk  
mount -t jffs2 -o ro,noatime /dev/mtdblock1 /mnt/flashdisk  
cd /mnt/flashdisk
```
- 4) In the `/mnt/flashdisk` directory, execute the following commands:
 - a) If the chassis type is GQS-G30CHASF-00, execute:

```
/sbin/mkfs.ext4 /dev/sda1
```

Otherwise, execute:

```
/sbin/mkfs.ext4 /dev/mmcblk0p1
```
 - b) `./bcm.init`
 - c) `./ed_ip <NE ip address> <NE netmask> LCI <Gateway ip address> <NE ip address>` and `<NE netmask>` are the IP address assigned to the module and the netmask of the IP address. `<Gateway ip address>` is the network gateway to the customer management network.

Example:

```
./ed_ip 10.2.0.1 255.255.0.0 LCI 10.2.0.52
```

- d) `./copy_rfile_ext4 <Remote FTP server ip address> 21 <FTP username> <FTP password> <SW load path>`

Example:

```
./copy_rfile_ext4 10.2.132.138 21 userforbc DLh*Sw0d1  
GROOVE_G30_4.6.6_20240408
```

- e) `./install_sw`

5) Copy the following files:

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

6) Set the node to the FIPS mode with `fipsmode` set to `fips`:

```
./ed_sys fipsmode=fips
```

7) Execute the following commands:

```
sync  
./init_sys
```

- 8) After the module restarts, log in with the default user `cryptoadministrator`, and then change the passwords of the three default users: `backup-admin`, `administrator` and `cryptoadministrator`.
- 9) If deploying TACACS+ or RADIUS service is planned, configure the IPsec ESP tunnel to the AAA server. Otherwise, skip this step. IPsec configuration details can be found on the user manuals.

Manual zeroization

The Crypto Officer can zeroize the keys by performing CLI command `clear-database clear-type=ssp-zeroization`. The details of this command can be found in the *Groove G30 CLI User Manual*.

The keys can also be zeroized by pressing the reset button for longer than 30 seconds.

All the SSPs will be zeroized after the zeroization operation, and the system reboot indicates the zeroization operation is complete.

Switching between modes of operation

The Crypto Officer can switch the module between the FIPS approved mode and the FIPS 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 following CLI command is issued:

```
set security system-fips enabled
```

In FIPS approved mode of operation, the module will be switched to FIPS non-approved mode of operation if the following CLI command is issued:

```
set security system-fips disabled
```

Please note that when the module is switched between FIPS approved mode and FIPS non-approved 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 CLI User Guide*.

11.2 Administrator Guidance

The approved and non-approved security functions available to users are listed in section 2, the physical ports, and logical interfaces available to users are specified in section 3.1. The Approved and non-Approved modes of operation are specified in section 2.4. The algorithm-specific information is listed in section 2.7.

11.3 Non-Administrator Guidance

No specific Non-Administrator guidance.

11.4 End of Life

The following procedures should be followed for the secure sanitization of the module:

- 1) Log in to the module with the CO role and manually zeroize the SSPs.
- 2) Once the module reboots, log in with the CO role and execute the `clear-database` command with the `clear-type factory-default` option.
- 3) Power down the module.

12 Mitigation of other attacks

This section is not applicable. The module does not claim to mitigate any attacks beyond the FIPS 140-3 Level 1 requirements for this validation.