Infinera Corporation
mTera 8-slot Universal Transport Platform
FIPS 140-2 Non-Proprietary Security Policy Level 2 Validation

Module Version: FP5.1.2

Hardware Version: 81.71S-MTERA8-R6 with tamper-evident labels MKS-MSECTAPE-00

Version 1.11

June 21, 2021

EDITOR

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

Revision History

Version	Description	Date	By
0.1	Initial Version	11/06/2018	Xinyu Fang
1.0	First Revision to testing lab	12/21/2018	Xinyu Fang Xifang Zhang Ruiqin Weng
1.1	Updated based on the testing laboratory review comments	01/24/2019	Xinyu Fang Xifang Zhang Ruiqin Weng
1.2	Updated based on the testing laboratory review comments	02/19/2019	Xinyu Fang Xifang Zhang Ruiqin Weng
1.3	Updated based on the NIST review comments	03/13/2019	Xinyu Fang Xifang Zhang
1.4	Updated based on the NIST review comments	04/18/2019	Xinyu Fang Xifang Zhang
1.5	Updated based on the NIST review comments	02/11/2020	Xinyu Fang Xifang Zhang
1.6	Updated based on the NIST review comments	09/30/2020	Xinyu Fang
1.7	Updated based on the NIST review comments	02/23/2021	Xinyu Fang
1.8	Updated based on the NIST review comments	04/26/2021	Xinyu Fang
1.9	Updated based on the NIST review comments	05/14/2021	Xinyu Fang
1.10	Updated based on the NIST review comments	06/08/2021	Xinyu Fang
1.11	Updated based on the NIST review comments	06/21/2021	Xinyu Fang

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 Purpose

This is a non-proprietary Security Policy for the Infinera mTera 8-slot Universal Transport Platform (mTera8 UTP) Cryptographic Module. This Security Policy describes how the cryptographic module meets the requirements for a FIPS 140-2 level 2 validation as specified in the FIPS 140-2 standard. This Security Policy is part of the evidence documentation package to be submitted to the validation lab.

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

1.2 Scope

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

1.3 Security level

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

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

Table 1 – Security level per FIPS 140-2 Section

2 Cryptographic module specification

The Infinera mTera 8-slot Universal Transport Platform (mTera8 UTP) is a flexible and scalable universal transport platform that can dynamically adapt to changing traffic patterns and address multiple use cases. Its capacity ranges from 1.6Tbps to 4.0Tbps.

The mTera8 UTP cryptographic module offers a transport solution that combines SDN-ready, advanced ROADM capabilities with universal switching. Universal switching provides non-blocking grooming of multiple protocols on a single, programmable port enabling the ultimate in flexibility and adaptability as networks grow. The mTera8 UTP is a solution for dense metro, regional, or long-haul networks.

The cryptographic module is a multi-chip standalone module.

2.1 Cryptographic module boundary

The cryptographic boundary of mTera8 UTP is defined as the entire shelf with front door and rear cover.

The mTera8 front door is stuck with the label 1, label 2 and label 5 of tamper-evident labels for protection purpose, which acts as tamper-evident label. The serial debug port of SIOM is covered by the serial port cover which is installed by the four screws (refer to Figure 8 in Appendix A) and then stuck with label 3 and label 4 of tamper-evident labels to prevent the SIOM module from being accessed through the serial port.

Note that the label in the following steps refer to the tamper-evident label.

The module hardware model is shown as following:

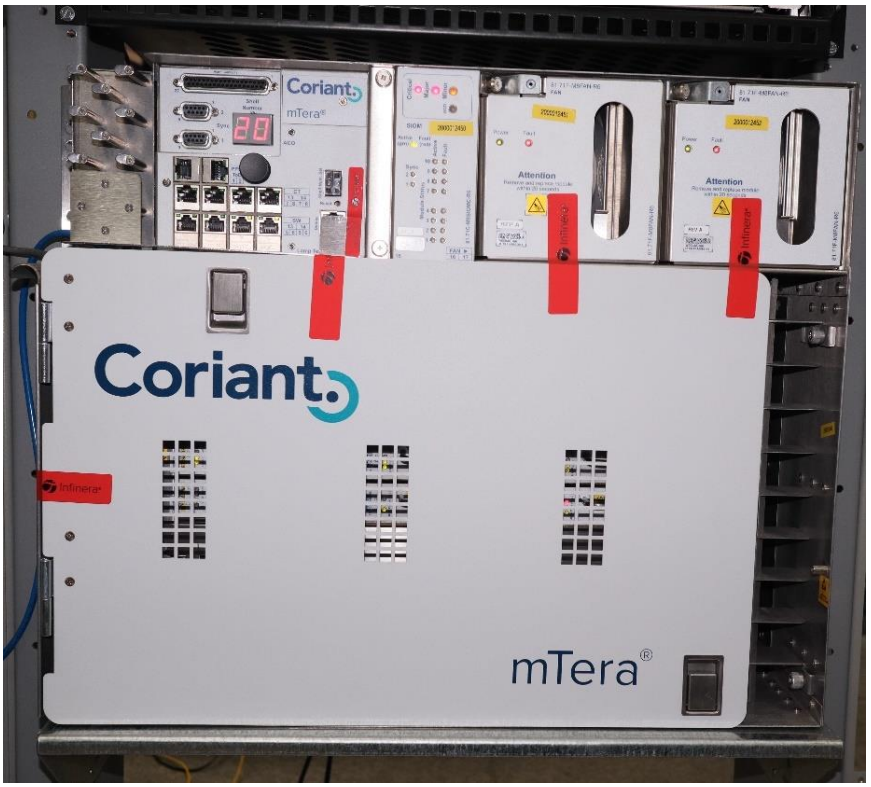

Figure 1 – Front view with door installed

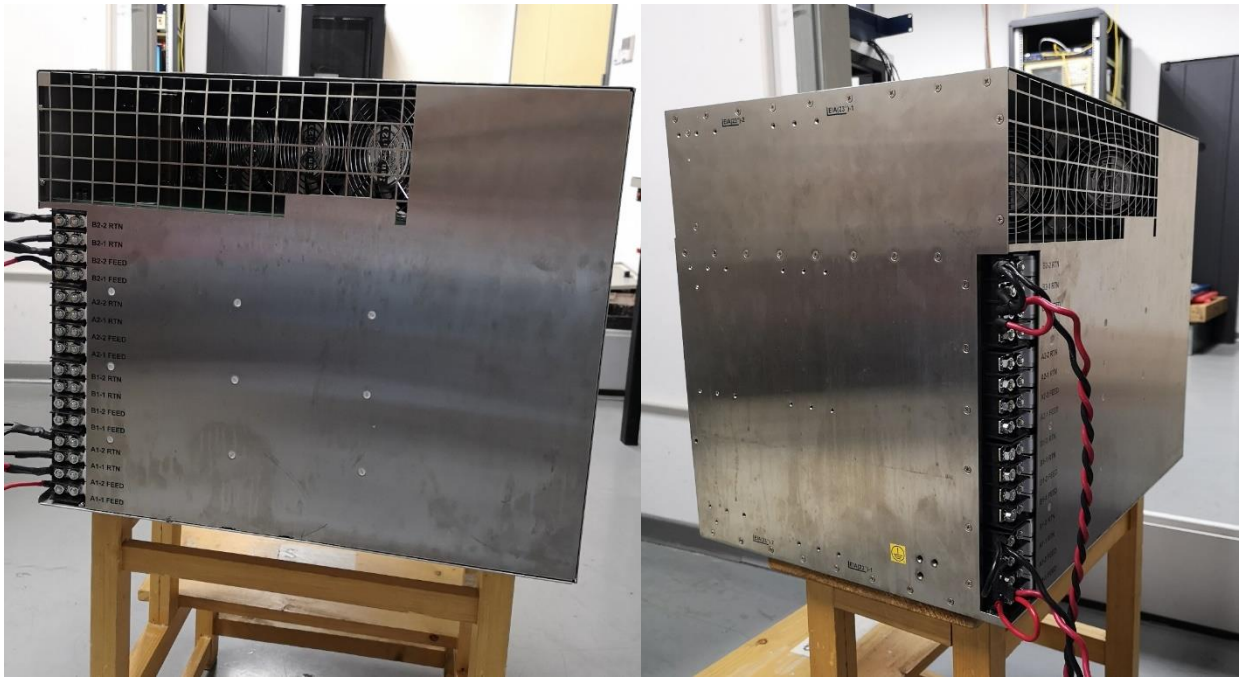

Figure 2 – Back view with rear cover

2.2 Hardware

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

The cryptographic module, mTera8 UTP, is composed of the following components:

mTera8 UTP chassis, controller card, fabric card, traffic interface card (component) and optical pluggable.

The mTera8 UTP chassis includes shelf, shelf door, and tamper-evident labels. STPM8 card is the controller card of mTera8 UTP. MFAB and MFAB2 are the fabric cards of mTera8 UTP. Traffic interface card includes OSM1S, OSM2S, OSM2C, OSM4SE, OSM4FE, OSM5CE, SSM2S, MRMN, OPF1CC, RS9, RS20 and MLAIC. Optical pluggable includes SFP, SFP+, CFP, CFP2 and OFP1.

2.3 Mode of operation

The mTera8 UTP Cryptographic Module has a FIPS approved security function mode of operation and a FIPS non-approved security function mode of operation.

The mTera8 UTP module will be placed into FIPS approved security function mode of operation when “FIPS” mode is set. When “NONFIPS” mode is set, the mTera8 UTP module will be placed into FIPS non-approved security function mode of operation.

Crypto Officers can set “FIPS” mode or “NONFIPS” mode by issuing TL1 commands to the module.

The procedure and detail TL1 commands are described in Section 11.4 Switching between FIPS approved security function mode of operation and FIPS non-approved security function mode of operation.

When the cryptographic module runs in FIPS approved security function mode of operation and the Crypto Officer switches the module to FIPS non-approved security function mode of operation, the CSPs will be zeroized automatically and mTera8 UTP module will restart into FIPS non-approved security function mode of operation.

When the cryptographic module runs in FIPS non-approved security function mode of operation and the Crypto Officer switches the module to FIPS approved security function mode of operation, the CSPs will be zeroized automatically and mTera8 UTP module will restart into FIPS approved security function mode of operation.

2.4 FIPS approved security functions

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

Algorithm	CAVP Cert. #
AES-CBC (128/256) AES-CTR (128/256) AES-ECB (128/256) AES-GCM (256) *Note1* AES-KW (256) for KTS	C537 (OpenSSL)
AES-CBC (128/192/256) AES-CTR (128/192/256) AES-ECB (128/192/256) AES-GCM (256) *Note1*	C538 (Kernel crypto)
AES-CTR (256) AES-ECB (256) AES-GMAC (key length:256 bits; tag length: 128 bits) *Note1* (Hardware encryption Engine from vendor Microsemi Corporation)	AES 3844 (Certificate from hardware vendor)
Counter DRBG (AES-256)	C537
ECDSA KeyGen (186-4) Curve: P-256, P-384, P-521 ECDSA KeyVer (186-4) Curve: P-256, P-384, P-521 ECDSA SigGen (186-4) Curve: P-256 with SHA2-256, SHA2-384, SHA2-512 Curve: P-384 with SHA2-256, SHA2-384, SHA2-512 Curve: P-521 with SHA2-256, SHA2-384, SHA2-512 ECDSA SigVer (186-4) Curve: P-256 with SHA-1, SHA2-256, SHA2-384, SHA2-512 Curve: P-384 with SHA-1, SHA2-256, SHA2-384, SHA2-512 Curve: P-521 with SHA-1, SHA2-256, SHA2-384, SHA2-512	C537
HMAC-SHA-1 (96/160) HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512	C537
HMAC-SHA-1 (96) HMAC-SHA2-256	C538
KAS-ECC CDH-Component: Curve: P-256, P-384, P-521 KAS-ECC Component: Ephemeral Unified: KAS Role: Initiator, Responder KDF without Key Confirmation: Parameter Set: EC: Hash Algorithm: SHA2-256, Curve: P-256 ED: Hash Algorithm: SHA2-384, Curve: P-384 EE: Hash Algorithm: SHA2-512, Curve: P-521	C537

Algorithm	CAVP Cert. #
KAS-FFC Component: dhEphem: KAS Role: Initiator, Responder KDF without Key Confirmation: Parameter Set: FB: Hash Algorithm: SHA2-256 FC: Hash Algorithm: SHA2-256	
KDF IKEv2 Capabilities: Initiator Nonce Length: 128-384 Responder Nonce Length: 128-384 Diffie-Hellman Shared Secret Length: 384 Derived Keying Material Length: 1056-2432 Hash Algorithm: SHA2-384 Capabilities: Initiator Nonce Length: 128-384 Responder Nonce Length: 128-384 Diffie-Hellman Shared Secret Length: 2048 Derived Keying Material Length: 1056-2432 Hash Algorithm: SHA-1, SHA2-256 KDF SNMP Password Length: 64-96 KDF SSH Cipher: AES-128, AES-192, AES-256 Hash Algorithm: SHA-1, SHA2-256, SHA2- 384, SHA2-512 KDF TLS *Note2* TLS Version: v1.2 Hash Algorithm: SHA2-384	C537
RSA KeyGen (186-4) Key Generation Mode: B.3.3 Modulo: 2048 Modulo: 3072 RSA SigGen (186-4) Signature Type: ANSI X9.31 Modulo: 2048 with SHA2-256, SHA2-384, SHA2-512 Modulo: 3072 with SHA2-256, SHA2-384, SHA2-512 Signature Type: PKCS 1.5 Modulo: 2048 with SHA2-256, SHA2-384, SHA2-512 Modulo: 3072 with SHA2-256, SHA2-384, SHA2-512 RSA SigVer (186-4) Signature Type: ANSI X9.31 Modulo: 2048 with SHA-1, SHA2-256, SHA2-384, SHA2-512 Modulo: 3072 with SHA-1, SHA2-256, SHA2-384, SHA2-512 Signature Type: PKCS 1.5 Modulo: 2048 with SHA-1, SHA2-256, SHA2-384, SHA2-512	C537

Algorithm	CAVP Cert. #
Modulo: 3072 with SHA-1, SHA2-256, SHA2-384, SHA2-512	
SHA-1 SHA2-256 SHA2-384 SHA2-512	C537
SHA-1 SHA2-256	C538
CKG – IG D.12 [SP.800-133r2] 5.1 Key Pairs generation using unmodified DRBG output for Digital Signature Schemes [SP.800-133r2] 5.2 Key Pairs generation using unmodified DRBG output for Key Establishment [SP.800-133r2] 6.1 The "Direct Generation" of Symmetric Keys generation using unmodified DRBG output [SP.800-133r2] 6.2.1 Symmetric Keys Generated Using Key-Agreement Schemes [SP.800-133r2] 6.4 Distributing Symmetric Keys using key wrapping	Vendor Affirmed

Table 2 – FIPS approved security functions

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

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

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

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

2.5 FIPS non-approved security functions allowed in FIPS mode

The mTera8 UTP cryptographic module implements the following non-approved but allowed algorithms in the FIPS 140-2 mode of operations:

- Diffie-Hellman (CAVP Cert. #C537) – provides 112 or 128 bits of encryption strength.
- Elliptic Curve Diffie-Hellman (CAVP Cert. #C537) – provides 192 bits of encryption strength.
- NDRNG – internal entropy source providing 512 bits of entropy to the DRBG.
- RADIUS over IPsec – remote user authentication.

2.6 FIPS non-approved security functions

The mTera8 UTP cryptographic module implements the following non-approved algorithms which are not permitted for use in the FIPS 140-2 mode of operations:

- MD5
- DES

3 Cryptographic module ports and interfaces

The mTera8 UTP cryptographic module provides a number of physical ports, and the physical ports can be categorized according to the following logical interfaces:

- Data Input Interface
- Data Output Interface
- Control Input Interface
- Status Output Interface
- Power Interface

	Name	Physical Ports	Quantity	Description	Logical Interface
mTera8 UTP Shelf Power Feeds	Power Feeds	PWR A1/A2/B1/B2	1	Power input	Power Interface
		PWR A1/A2/B1/B2 RTN	1	Power return	
Shelf Slot card (I/F)	OSM1S	SFP	32	Optical connections	Data Input Interface *Note1, Note3* Data Output Interface *Note1, Note3* Control Input Interface *Note2,Note3* Status Output Interface *Note2,Note3*
	OSM2S	SFP+	20	Optical connections	
	OSM2C	CFP	2	Optical connections	
	SSM2S	SFP	24	Optical connections	
		SFP+	6	Optical connections	
	OSM4SE	SFP+	40	Optical connections	
	OSM4FE	LC/PC	2	Optical connections	
	OSM5CE	CFP2	5	Optical module	
POL	CDC8D6	LC/PC	28	Optical connections	
Shelf Interface card (Optics)	MRMN	LC/PC	5	Optical connections	
		OFP1	1	POL - Coriant proprietary module form factor	
	OPF1CC	OFP1	3	POL - Coriant proprietary module form factor	
	MLAIC	LC/PC	8	Optical connections	
	RS9	LC/PC	28	Optical connections	
		RJ45	3	1-wire bus interface	Data Input Interface Data Output Interface
	RS20	LC/PC	52	Optical connections	Data Input Interface *Note3* Data Output Interface *Note3* Control Input Interface *Note2, Note3* Status Output Interface *Note2, Note3*
		RJ45	3	1-wire bus interface	Data Input Interface

	Name	Physical Ports	Quantity	Description	Logical Interface
					Data Output Interface
mTera8 UTP Shelf IO card	SIOM	RJ45	1	Serial over 10/100Base-T	Data Input Interface Data Output Interface
		Shelf ID switch	1	Not functional	N/A
		ACO Button	1	Alarm cutoff button to clear the alarms	Control Input Interface
		Lamp Test push button	1	NE Alarm LEDs and ACO LED test	Control Input Interface
		RJ45	4	Control & Timing (Not functional)	N/A
		RJ45	4	Management interface 10/100/1000Base-T	Control Input Interface Status Output Interface
		DB-37	1	Alarm IO	Control Input Interface Status Output Interface
		DB-9	2	BITS	Control Input Interface Status Output Interface
		RJ45	2	PPS/TOD	Data Input Interface Data Output Interface
	STPM8	USB	1	Not functional	N/A
		RJ45	1	Local Craft Station	Control Input Interface Status Output Interface
		RJ45	2	CT-1&CT-2 (Not functional)	N/A
		SFP+	2	Not functional	N/A

Table 3 – Ports and logical Interfaces

Note 1: mTera8 UTP provides data encryption functions (CAVP #AES-3844, see Table 2 – FIPS Approved Security Functions) on OSM5CE, OSM4SE and OSM4FE cards.

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

Note 3: The "data input interface" and "control input interface" are different from "data output interface" and "status output interface" on message transmission direction. The fiber channels from the module to the outside are the "data output interfaces" and "control output interfaces". The fiber channels from the outside to the module are the "data input interfaces" and "control input interfaces". In a fiber channel, the control input interface or status output interface occupies the OH (overhead) bytes of the channel while data input interface or data output interface occupies the data bytes of the channel.

4 Roles, services and authentication

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

4.1 Authorized roles

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

Multiple concurrent operators are allowed to this module. The maximum number of concurrent operators is 128. They are identified and authorized by username and password. The multiple concurrent operators can be in CO role and in User role.

Only the operator with CO role has the ability to change roles. Modifications of role will be applied following the next login session of the same user.

The module does not support a Maintenance Role.

4.2 Services

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

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

R – Read, the CSP is read.

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

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

Service	CO	User	Description	Input	Output	CSP and Type of Access
Initialize the module	√	√	Initialize the module	Command	Status output	Master key – R/W/X
Configure and show the system	√	√	Configure and show system settings	Command and parameters	Command response	None
Set FIPS mode	√	√	Switch from FIPS-approved security function mode to FIPS-non approved security function mode	Command and parameters	Command response	Clear plaintext CSP
show FIPS mode	√	√	Switch from FIPS-approved security function mode to FIPS-non approved security function mode	Command and parameters	Command response	Clear plaintext CSP
Generate asymmetric key pair	√		Generate the asymmetric key pair for certificate and SSH	Command and parameters	Command response	ECDSA or RSA Private Key – W ECDSA or RSA Public Key – W
Manage CA certificate, root	√		Generate CSR, Export CSR,	Command and	Command response	Certificate private key and public key –

Service	CO	User	Description	Input	Output	CSP and Type of Access
CA certificate and CRL			Import signed CA certificate, Import root CA certificate, Import CRL	parameters		R/X
Create data encryption / decryption service	√		Encrypt or decrypt user data, and manage the data encryption/decryption key	Command and parameters	Command response	Data encryption AES key – X
Manage TLS session for data traffic	√	√	Build up TLS session for data traffic	Command and parameters	Command response	TLS session Key – W/X
Monitor alarms	√	√	Monitor alarms for diagnostic purpose	Command	Status output	None
View system logs	√	√	View system status messages in historical alarm log and provisioning log	Command	Status output	None
Perform device diagnostics	√	√	Test the module during operation	Command and parameters	Command response and status via log and LEDs	None
Upgrade application firmware, FPGA image and chipset firmware *Note1*	√	√	Upgrade the application firmware, FPAG image and chipset firmware using RSA signature verification	Command and parameters	Command response and status output	RSA Public Key – X
IPsec	√		Secure, rekeying, communications between the module and Management system over DCN	Command and parameters	Command response and Status output	Certificate private key and public key – X Volatile, internal, generated, symmetric authentication and encryption keys with perfect forward secrecy - X
Zeroize	√		Zeroize the master key	Command	Command response	Please refer to the Section *11.3 Key Zeroization* for detail CSPs.
Perform on demand self-tests	√	√	Perform self-tests on demand	Command	Status output	None
Power on self-tests			Perform self-tests when system is power on; services not requiring an authorized role.		Status output	None
Perform Packet Service	√	√	Perform packet related service provisioning and status retrieval.	Command	Status output	None
Perform L0 optical service	√	√	Perform L0 optical related service provisioning and status retrieval.	Command	Status output	None
Perform L1 OTN service	√	√	Perform L1 OTN related service provisioning and status retrieval.	Command	Status output	None
SSH	√	√	Access the module through	Command	Status	SSH keys and user

Service	CO	User	Description	Input	Output	CSP and Type of Access
			Secure Shell		output	credentials – R
Key Wrap	√		Wrap the key for ODU encryption key during synchronization to peer		Status output	ODU encryption key – R
SNMPv3	√	√	SNMPv3 service	Command	Status output	SNMP privacy and authentication passphrases – R
Controller switching	√	√	Switch the active and standby controllers	Command	Status output	None
Diffie-Hellman	√	√	Provides 112 or 128 bits of encryption strength.	N/A	N/A	Shared secret-R/W/X
Elliptic Curve Diffie-Hellman	√	√	Provides 192 bits of encryption strength.	N/A	N/A	Shared secret-R/W/X
NDRNG			Provides 512 bits of entropy to the DRBG. Services not requiring an authorized role.	N/A	N/A	Shared secret-W
RADIUS over IPsec	√	√	Remote User authentication	Command and parameters	Command response	Shared secret-R/X

Table 4 – FIPS approved services

Note 1: Only the CMVP validated firmware version is allowed to be used.

Service	CO	User	Description	Input	Output	CSP and Type of Access
MD5	√	√	Message Digest used for RADIUS and SNMP protocol	N/A	N/A	N/A
DES	√	√	The SNMP privacy protocol	N/A	N/A	N/A

Table 5 – FIPS non-approved services

4.3 Authentication

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

4.3.1 CO and user authentication

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

The following rules apply for the password complexity:

- Password length must be 8 characters minimum
- At least 3 of the 4 following character types must be present:
  - Numeric character, lowercase alphabetical character, uppercase alphabetical character, special character.
- Special character consists of any of the following: ! # $ % & @ ^*
- The Password must not include more than 2 consecutive repetitions of the same character.
- UID (UserId) must not be contained in password (case insensitive).

If 6 integers, 1 alphabetical character and 1 special character are used for an 8 digit PIN, the probability of randomly guessing the correct sequence is 1 in 245,643,840(this calculation is based on the assumption that the typical standard American QWERTY computer keyboard has 10 Integer digits, 52 alphabetic characters, and 8 special characters to choose from in total. The calculation should be10x9x9x9x9x9x52x8= 245,643,840).

Therefore, the associated probability of a successful random attempt is approximately 1 in 245,643,840, which is less than the 1 in 1,000,000 required by FIPS 140-2.

The login will be locked out for the operator (the period of the lockout is user defined, max 300 seconds, min 60 seconds, which can be set by Crypto Officer through TL1 command ED-SECU-SYS), when the maximum number of consecutive and invalid attempts (maximum is 9) happen. So the associated probability of a successful random attempt during a one-minute period is less than $9/245,643,840 = 3.66384x10^{-8}$, which is less than one in 100,000.

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

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

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

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

4.3.2 SSH authentication

In FIPS mode, users login to the module with secure shell (SSH). The module works as SSH server. It supports user password based and key based SSH authentications. RSA-2048 is supported for key based SSH authentication.

RSA-2048 has modulus size of 2048 bits, which providing 112 bits of strength. It provides the probability of a successful random obtaining the RSA key is 1 in 2^{112}, 1.92E-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 $9/2^{112}$, 1.73E-33, which is much less than one in 100,000 that is required by FIPS 140-2.

5 Physical security

To operate in FIPS approved security function mode the tamper-evident labels shall be installed on the shelf with door installed as shown in Appendix A.

5.1 Physical security mechanisms as required by FIPS 140-2

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

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

- Production-grade components and production-grade opaque enclosure.
- Tamper-evident labels. Refer to “Procedure 2: Install the tamper-evident labels” of Appendix A for detailed instructions on tamper-evident label placement.
- Service cards are installed in slots of shelf.
- All unpopulated slots are equipped with filler cards.

Tamper-evident labels

Tamper-evident labels shall be installed for the module to operate in a FIPS-approved security function mode of operation.

Two sizes of tamper-evident labels are used, the 2.363 inch* 0.394 inch size and the 3.150 inch* 0.788 inch size (the two sizes of labels share one Infinera PN: MKS-MSECTAPE-00). The following graphics illustrate the tamper-evident labels, drawing in inches.

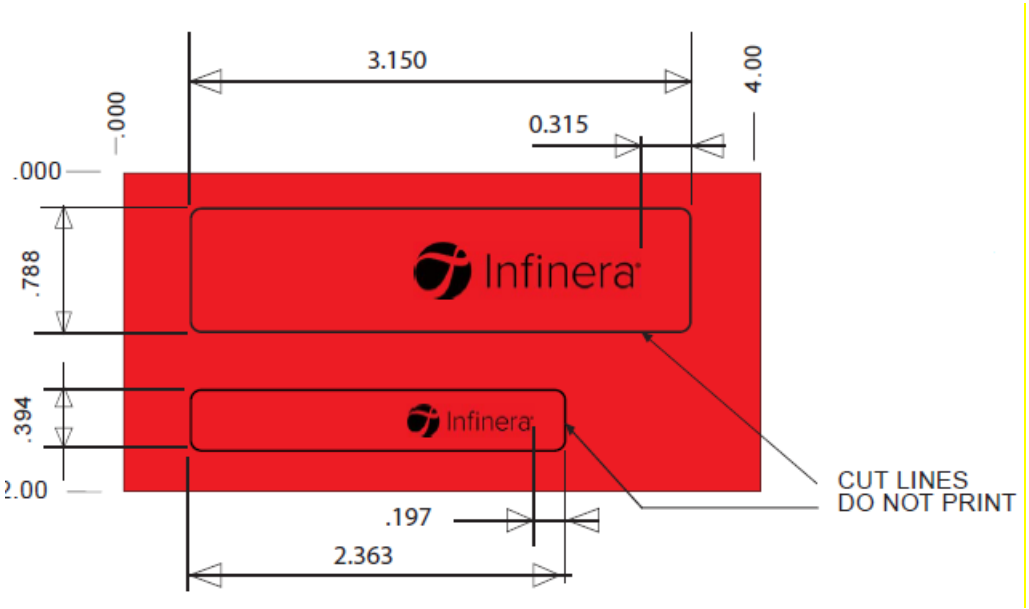

Figure 3 – Tamper-evident label

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

Figure 4 - Tamper-evident label: intact

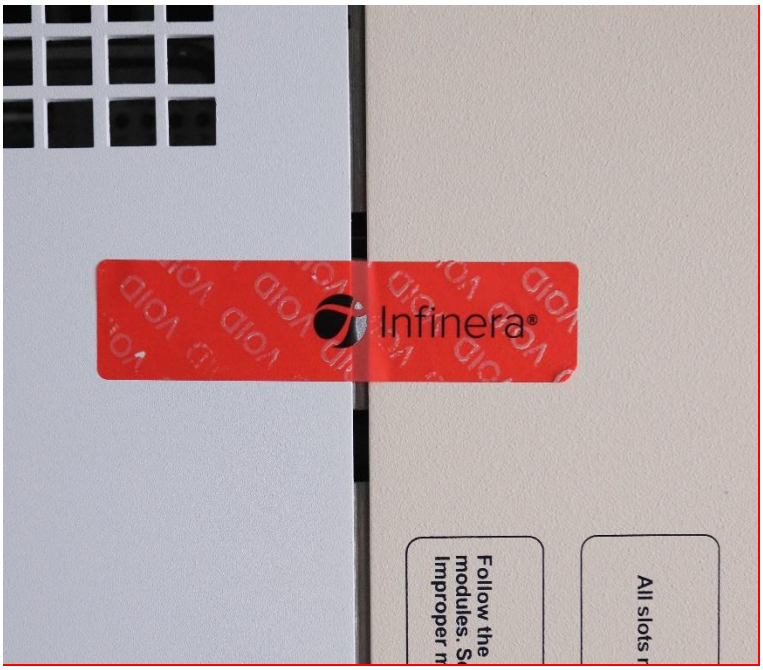

Figure 5 - Tamper-evident label: broken (normal view)

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

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

Inspect labels

The Crypto Officer is also responsible for inspecting the tamper-evident labels on the shelves at least every 30 days. If any evidence of tampering is observed on the tamper-evident seals, the module shall be considered to be in a non-compliant state.

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

Detailed procedures on affixing labels for mTera8 UTP is given in appendix A.

6 Operational environment

The mTera8 UTP module does not contain a modifiable operational environment.

7 Cryptographic key management

7.1 Cryptographic key and critical security parameters

The mTera8 UTP module has a set of cryptographic keys, cryptographic key components and CSPs. The plain text keys and CSPs can be zeroized by the Crypto Officer, and the zeroization operation will overwrite RAM that stores the temporary keys.

The mTera8 UTP module has a master key stored on the EEPROM of the system, which is initialized when the module is switched from FIPS non-approved security function mode to FIPS approved security function mode and zeroized automatically when the module is switched from FIPS approved security function mode to FIPS non-approved security function mode by the Crypto Officer. The master key in the EEPROM will be rewritten to “all zero”.

The mTera8 UTP module has plain text keys in the SRAM space on FPGA for the ODU encryption function. The keys will also be zeroized when the Crypto Officer manually zeroizes the keys or when the module is switched from FIPS approved security function mode to FIPS non-approved security function mode by the Crypto Officer.

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

In the FIPS approved security function mode of operation, the mTera8 UTP module uses HW RNG (K82) to generate true random bits and sends them to DRBG as its seed. These seed values are temporarily stored in RAM and are zeroized by power cycling the module. These values are not accessible to any user. DRBG will feed random numbers to all the other cryptographic functions. The module implements SP 800-90A DRBG Section 11.3 Health tests

“ODU encryption AES-CTR key” and “ODU encryption AES-GMAC key” in the table below can be transported out of the mTera8 UTP module with AES-KW key wrapping algorithm. The AES keys for key wrap are from the Diffie-Hellman or Elliptic Curve Diffie-Hellman key exchange between the mTera8 UTP module and its peers. Since keys being wrapped are keys of AES-CTR-256 and AES-GMAC-256, the cryptographic strength of the encryption key is equal to the cryptographic strength of the keys being wrapped.

The mTera8 UTP module supports the following cryptographic keys, cryptographic key components, CSPs and Public keys.

Key Item	Key function	Key Generation Method	Key Output	Key Storage	Key Zeroization
IKE2 HMAC	Session key integrity check	Generated internally / key exchange	No output	RAM	Reboot Zeroization on rekeying
ESP HMAC	Session key authentication	Generated internally / key exchange	No output	RAM	Reboot Zeroization on rekeying
IKE2 AES	Session key encryption	Generated internally / key exchange	No output	RAM	Reboot Zeroization on rekeying
ESP AES	Session key encryption	Generated internally / key exchange	No output	RAM	Reboot Zeroization on rekeying
X.509 auth.	X.509 certificates	Externally provided	CSR upload	SD Card with AES encryption	Zeroization on manual delete
Key from DRBG	Key generated by DRBG for all the cryptographic functions	Generated by DRBG	No output	RAM	FIPS/NONFIPS mode switching; Manual Zeroization ;Power cycle
Seed to DRBG	Used for function requiring random number	Generated internally by HW(K82)	No output	RAM	FIPS/NONFIPS mode switching; Manual Zeroization ;Power cycle
DRBG V and key values	Internal state values for the DRBG	Generated by DRBG	No output	RAM	FIPS/NONFIPS mode switching; Manual Zeroization ;Power cycle
Master key	Key to encrypt the other Key/CSP	Generated internally by DRBG	No output	EEPROM	FIPS/NONFIPS mode switching; Manual Zeroization
PID	User password	Input by TL1 command	No output	SD Card with AES encryption	FIPS/NONFIPS mode switching; Manual Zeroization
Elliptic Curve Diffie-Hellman private key	Elliptic Curve Diffie-Hellman private key	Generated internally	No output	RAM	FIPS/NONFIPS mode switching; Manual Zeroization ;Power cycle
Elliptic Curve Diffie-Hellman public key	Elliptic Curve Diffie-Hellman public key	Generated internally	output	RAM	FIPS/NONFIPS mode switching; Manual Zeroization ;Power cycle
Elliptic Curve Diffie-Hellman shared secret	Elliptic Curve Diffie-Hellman shared secret	Generated internally	No output	RAM	FIPS/NONFIPS mode switching; Manual Zeroization ;Power cycle
Diffie-Hellman private key	Diffie-Hellman private key	Generated internally	No output	RAM	FIPS/NONFIPS mode switching; Manual Zeroization ;Power cycle
Diffie-Hellman public key	Diffie-Hellman public key	Generated internally	output	RAM	FIPS/NONFIPS mode switching; Manual Zeroization ;Power cycle
Diffie-Hellman shared secret	Diffie-Hellman shared secret	Generated internally	No output	RAM	FIPS/NONFIPS mode switching; Manual Zeroization; Power cycle
TLS(DHE-RSA) preMaster secret	TLS preMaster secret	Derived from DH	No output	RAM	FIPS/NONFIPS mode switching; Manual Zeroization; Power cycle
TLS(DHE-RSA) Master Secret	TLS Master Secret	Derived from DH	No output	RAM	FIPS/NONFIPS mode switching; Manual Zeroization; Power cycle
TLS(DHE-RSA) session key	TLS session key	Derived from DH	No output	RAM	FIPS/NONFIPS mode switching; Manual Zeroization; Power cycle
TLS(ECDHE-ECDSA) preMaster secret	TLS preMaster secret	Derived from ECDH	No output	RAM	FIPS/NONFIPS mode switching; Manual Zeroization; Power cycle
TLS(ECDHE-ECDSA) Master Secret	TLS Master Secret	Derived from ECDH	No output	RAM	FIPS/NONFIPS mode switching; Manual Zeroization; Power cycle
TLS(ECDHE-ECDSA) session key	TLS session key	Derived from ECDH	No output	RAM	FIPS/NONFIPS mode switching; Manual Zeroization; Power cycle
System private Key for TLS and IPsec - RSA	System private Key - RSA	RSA Private key for generation of signatures, authentication and key establishment; Generated through command; Used to export CSR; Associated with NE certificate	No output	SD Card with AES encryption	FIPS/NONFIPS mode switching; Manual Zeroization;

Key Item	Key function	Key Generation Method	Key Output	Key Storage	Key Zeroization
System public Key for TLS and IPsec - RSA	System public Key -RSA	Generated from System private Key in running time if requested by security functions	output	SD Card with AES encryption	FIPS/NONFIPS mode switching; Manual Zeroization; Power cycle
System private Key for TLS and IPsec - ECDSA	System private Key - ECDSA	ECDSA Private key for generation of signatures, authentication and key establishment; Generated through command; Used to export CSR; Associated with NE certificate	No output	SD Card with AES encryption	FIPS/NONFIPS mode switching; Manual Zeroization;
System public Key for TLS and IPsec - ECDSA	System public Key - ECDSA	Generated from System private Key in running time if requested by security functions	output	SD Card with AES encryption	FIPS/NONFIPS mode switching; Manual Zeroization; Power cycle
TLS HMAC - SHA1	TLS HMAC	TLS integrity and authentication session keys	No output	RAM	FIPS/NONFIPS mode switching; Manual Zeroization; Power cycle
TLS HMAC - SHA384	TLS HMAC	TLS integrity and authentication session keys	No output	RAM	FIPS/NONFIPS mode switching; Manual Zeroization; Power cycle
SNMPv3 Privacy Passphrase	SNMPv3 Privacy secret	Input by TL1 command	No output	SD Card with AES encryption	FIPS/NONFIPS mode switching; Manual Zeroization;
SNMPv3 Authentication Passphrase	SNMPv3 Authentication secret	Input by TL1 command	No output	SD Card with AES encryption	FIPS/NONFIPS mode switching; Manual Zeroization;
SNMPv3 Privacy key	SNMPv3 Privacy Key	Generated internally by Privacy passphrase	No output	RAM	FIPS/NONFIPS mode switching; Manual Zeroization;
SNMPv3 Authentication key	HMAC SHA1 key	Generated internally by Authentication passphrase	No output	RAM	FIPS/NONFIPS mode switching; Manual Zeroization;
ODU encryption AES-CTR key	ODU encryption AES-CTR key	Got from DRBG	wrapped by AES	RAM & SD Card with AES encryption	FIPS/NONFIPS mode switching; Manual Zeroization;
ODU encryption AES-GMAC key	ODU encryption AES-GMAC key	Got from DRBG	wrapped by AES	RAM & SD card with AES encryption	FIPS/NONFIPS mode switching; Manual Zeroization;
Key Wrap Key	Key Wrap Key for ODU encryption keys	Derived from DH or ECDH	No output	RAM	FIPS/NONFIPS mode switching; Manual Zeroization;
SSHv2 server private key - ECDSA	SSH Key	Generated through command (ED-TCPIP)	No output	SD Card with AES encryption	FIPS/NONFIPS mode switching; Manual Zeroization;
SSHv2 server public key - ECDSA	SSH public Key	Generated through command (ED-TCPIP)	output	SD Card with AES encryption	FIPS/NONFIPS mode switching; Manual Zeroization;
SSHv2 server private key - RSA	SSH Key	Generated through command (ED-TCPIP)	No output	SD Card with AES encryption	FIPS/NONFIPS mode switching; Manual Zeroization;
SSHv2 server public key - RSA	SSH public Key	Generated through command (ED-TCPIP)	output	SD Card with AES encryption	FIPS/NONFIPS mode switching; Manual Zeroization;
SSH session Key	SSH Encryption AES Key	Derived from DH/ECDH for AES-256/128-CBC/CTR/GCM	No output	RAM	FIPS/NONFIPS mode switching; Manual Zeroization; Power cycle
SSH authentication key	SSH authentication key used by message authentication function	Derived by SSH key agreement	No output	RAM	FIPS/NONFIPS mode switching; Manual Zeroization; Power cycle
RADIUS shared secret	RADIUS shared secret	Input by TL1 command	No output	SD Card with AES encryption	FIPS/NONFIPS mode switching; Manual Zeroization;
CSR for TLS and IPsec(including System public Key) - ECDSA	CSR (including System public Key) - ECDSA	Generated from System private Key in running time if requested by security functions	output	RAM	FIPS/NONFIPS mode switching; Manual Zeroization; Power cycle
NE local certificate for TLS and IPsec(including System public Key) - ECDSA	NE local certificate (including System public Key) Key - ECDSA	Downloaded from external file server	No output	SD Card with AES encryption	FIPS/NONFIPS mode switching; Manual Zeroization; Power cycle
CSR for TLS and IPsec (including	CSR (including System public Key) - RSA	Generated from System private Key in running time if requested by security functions	output	RAM	FIPS/NONFIPS mode switching; Manual Zeroization; Power cycle

Key Item	Key function	Key Generation Method	Key Output	Key Storage	Key Zeroization
System public Key) - RSA					
NE local certificate for TLS and IPsec(including System public Key) - RSA	NE local certificate (including System public Key) - RSA	Downloaded from external file server	output	SD Card with AES encryption	FIPS/NONFIPS mode switching; Manual Zeroization; Power cycle
CA certificate for TLS and IPsec - RSA	CA certificate - RSA	Downloaded from external file server	No output	SD Card with AES encryption	FIPS/NONFIPS mode switching; Manual Zeroization; Power cycle
CA certificate for TLS and IPsec - ECDSA	CA certificate - ECDSA	Downloaded from external file server	No output	SD Card with AES encryption	FIPS/NONFIPS mode switching; Manual Zeroization; Power cycle
Data integrity check - public RSA key	Data integrity check - public RSA key	hardcoded in the firmware image	No output	SD Card with AES encryption	-

Table 6 – Critical security parameters and public keys

8 Electromagnetic interference/compatibility (EMI/EMC)

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

9 Self-tests

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

If self-tests fail, the mTera8 UTP module will go into an error state and the FIPS_SELFTEST_FAIL alarm will be raised. In the error state, all data output via the data output interface will be inhibited.

9.1 Power-up self-tests

Each time this cryptographic module is powered up, it tests that the cryptographic algorithms still operate correctly and that sensitive data have not been damaged. Restarting the cryptographic module provides a means by which the operator can perform the power-up self-tests on demand.

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

Power-up self-tests include:

- Algorithm self-tests
  - OpenSSL (CAVP Cert. #C537)

- AES-CBC (128/256) Encrypt/Decrypt KAT
- AES-CTR (128/256) Encrypt/Decrypt KAT
- AES-ECB (128/256) Encrypt/Decrypt KAT
- AES-GCM (256) Encrypt/Decrypt KAT
- AES-KW (256) Encrypt/Decrypt KAT
- DH 2048 bits KAT
- DRBG KAT with health test
- ECDSA Pair-Wise Consistency Test
- ECDH P-256/384/521 KAT
- HMAC-SHA1/ HMAC-SHA-256/384/512 KAT
- KDF IKEv2 KAT
- KDF SNMP KAT
- KDF SSH KAT
- KDF TLS KAT
- RSA Pair-Wise Consistency Test
- SHA-1/ SHA2-256/384/512 KAT

▪ Linux Kernel (CAVP Cert. #C538)

- AES-CBC (128/192/256) Encrypt/Decrypt KAT
- AES-CTR (128/192/256) Encrypt/Decrypt KAT
- AES-EBC (128/192/256) Encrypt/Decrypt KAT
- AES-GCM (256) Encrypt/Decrypt KAT
- HMAC-SHA-1/SHA2-256 KAT
- SHA-1/SHA2-256 KAT

▪ Line Card (CAVP AES Cert. #3844)

- AES-CTR (256) Encrypt/Decrypt KAT
- AES-ECB (256) Encrypt/Decrypt KAT
- AES-GMAC (256) Encrypt/Decrypt KAT

- Firmware images integrity test with CRC32 (Main controller/Line card)

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

9.2 Conditional self-tests

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

- Pair-wise consistency test
  - RSA Pair-Wise Consistency Test
  - ECDSA Pair-Wise Consistency Test

- Firmware load integrity test with RSA signature
- Continuous random number generator test for DRBG
- Continuous random number generator test for NDRNG
- SP 800-90A DRBG Section 11.3 health test

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

10 Mitigation of other attacks

The module does not claim to mitigate any other attacks.

11 Security operation

The mTera8 UTP module meets Level 2 requirements of FIPS 140-2. The sections below describe how to place and keep the module in the FIPS-approved security function mode of operation.

11.1 Initial setup

1. The Crypto Officer must follow the [mTera SA&OP], and connect the serial interface and LCI interface to the craft station PC.
2. The Crypto Officer downloads the firmware images from the craft station PC, according to the guide of the [mTera SA&OP].
3. The Crypto Officer enters the basic commissioning setup page of the craft station, and install firmware to mTera8 UTP, make sure the “FIPS” check box is checked.
4. The Crypto Officer logins the mTera8 UTP module with the initial CO TL1 user name and user password, shipped along with the module.
5. The Crypto Officer installs the cards, pluggables, fibers and cables according to the [mTera Install].
6. The Crypto Officer applies the following installation of shelf door and tamper-evident labels following the instruction of Appendix A.

- Install the shelf door following the procedure of chapter 8 of installation manual [mTera Install].
- Install the tamper-evident labels

11.2 IPsec initial setup

The following operation should be after initial setup and the basic DCN provisioning should be done by the Crypto officer according to [mTera SA&OP]. The details of the commands in the following steps can be found in the [mTera TL1]. All the operations should be done by the Crypto Officer.

1. Connects LCI interface to the craft station PC and login mTera8 UTP from craft station PC.
2. Create Distinguished Name by command ENT-DN.
3. Create key pair by command ENT-ASYMKEY.
4. Export CSR associated with distinguished name and key pair created in the above steps to an SFTP server located in the DCN network by command OPR-EXPORT-CSR.
5. Download and install CA root certificate(s) from the SFTP server by command ENT-CERT.
6. Download and install the mTera8 UTP module certificate after CSR is signed by the certificate authority from the SFTP server by command ENT-CERT.
7. Create IPsec application entity associated with the above certificate by command ENT-ENCAPP.
8. Create IPsec peer entity associated with the above IPsec application command ENT-ENCPEER.
9. Create SPD associated with the above IPsec peer entity.

11.3 Key zeroization

The Crypto Officer can zeroize the keys by perform TL1 command OPR-FIPS-ZEROIZECSP. The details of this command can be found in the [mTera TL1].

After the zeroization command is executed, the master key in the EEPROM will be zeroized, and the mTera8 UTP module will reboot automatically to clean the other keys in the RAM.

11.4 Switching between FIPS approved security function mode of operation and FIPS non-approved security function mode of operation

The Crypto Officer can switch the mTera8 UTP module between FIPS approved security function mode and non-approved security function mode of operation by executing TL1 command ED-SECU-SYS.

In FIPS non-approved security function mode of operation, the mTera8 UTP module will be switched to FIPS approved security function mode of operation if the TL1 command ED-SECU-SYS is issued with parameter SECURE=FIPS.

In FIPS approved security function mode of operation, the mTera8 UTP module will be switched to FIPS non-approved security function mode of operation if the TL1 command ED-SECU-SYS is issued

with parameter SECURE=NONFIPS.

Please note that when the mTera8 UTP module is switched between FIPS approved security function mode and non-approved security function mode of operation, key zeroization and system restart will be automatically performed.

The current mode of operation can be retrieved by TL1 command RTRV-SECU-SYS. Details of these two commands can be found in the [mTera TL1].

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

There are three AES-GCM implementations and one AES-GMAC implementation on the module.

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

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

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

The module's hardware (ODU encryption) AES-GMAC implementation conforms to IG A.5, scenario #4. The hardware AES-GMAC 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-GMAC re-key interval (86400 seconds).

For each ODU frame, the IV is composed of 32bit nonce + 26bit unused + 30bit MFI + 8bit MFAS. MFI

is the multi-frame index and it increases 1 for every multi-frame. 256 ODU frames compose one multi-frame and MFAS increases 1 for each frame. Total 38 bits are used for ODU frame counter. The count always begins at zero for both MFI and MFAS when a new key is generated. In one second, the maximum multi-frame number is 3344. So in one maximum ODU encryption interval (86400s), the maximum ODU frame number is 86400*3344*256 =73,963,929,600, which is less than 2^38. It means in a maximum ODU encryption interval, the ODU frame counter (MFI+MFAS) will never repeat. The encryption key and nonce counter are generated from DRBG so possibility of repeat the key/IV pair is $2^{-256} * 2^{-32} = 2^{-288}$.

The key replacement period is configurable from 3600 seconds to 86400 seconds (24 hours). The key replacement period is translated to maximum multi-frame number which is provisioned to both encryption ends in chip set. If the key replacement period is set the 24 hours, the maximum multi-frame value for an AES key will be 86400*3344=288,921,600. MFI, which increases for each multi-frame, is carried over the header of ODU frame. In the encryption side, once the MFI value gets to the pre-provisioned maximum multi-frame number, key rotation will be triggered for next frame, and MFI will be started from 0. In the decryption ends, once the MFI in receiving ODU frame gets to the pre-provisioned maximum multi-frame number, key rotation will be triggered for next frame.

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

12 References

[FIPS 140-2]	*Security Requirements for Cryptographic Modules* *https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf*
[FIPS 140-2 DTR]	*Derived Test Requirements for FIPS PUB 140-2, Security Requirements for Cryptographic Modules* *https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/fips140-2/fips1402dtr.pdf*
[FIPS 140-2 IG]	*Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program* *https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/fips140-2/fips1402ig.pdf*
[mTera SA&OP]	*mTera Universal Transport Platform System Administration and Operation* authorized customer can download the documents from technical support website: https://infinera.lightning.force.com/lightning/n/Downloads2

[mTera Install]	*mTera Universal Transport Platform installation* authorized customer can download the documents from technical support website: https://infinera.lightning.force.com/lightning/n/Downloads2
[mTera TL1]	*mTera Universal Transport Platform TL1 Specification* authorized customer can download the documents from technical support website: https://infinera.lightning.force.com/lightning/n/Downloads2

13 Acronyms

ACO	Alarm Cut Off
AES	Advanced Encryption Standard
CA	Certificate Authority
CBC	Cipher Block Chaining
CFP	C Form-factor Pluggable
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CRC32	32-bit Cyclic Redundancy Check
CSP	Critical Security Parameter
CSR	Certificate Signing Request
DCC	Data Communication Channel
DCN	Data Communication Network
DES	Data Encryption Standard
DH	Diffie-Hellman
DHE	Diffie-Hellman Ephemeral
DRBG	Deterministic Random Bits Generator
DWDM	Dense Wavelength Division Multiplexing
ECB	Electronic Codebook Book
ECDSA	Elliptic Curve Digital Signature Algorithm
ECDH	Elliptic Curve Diffie-Hellman
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral

EEROM	Electrically Erasable, Programmable Read Only Memory
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ESP	Encapsulating Security Payload
FCC	Federal Communication Commission
FIPS	Federal Information Processing Standard
FPGA	Field Programmable Gate Array
GCC	General Communication Channel
GCM	Galois/Counter Mode
GMAC	Galois Message Authentication Code
HMAC	Keyed-Hash Message Authentication Code
IP	Internet Protocol
IPsec	Internet Protocol Security
KAS	Key Agreement Schemes
KDF	Key Derivation Function
KTS	Key Transportation Scheme
LCI	Local Craft Interface
MD5	Message-Digest Algorithm
MFAS	MultiFrame Alignment Signal
MFI	Multiframe Indicator
NDRNG	Non-deterministic Random number generators
ODU	Optical Data Unit
OFP1	Optical Form Factor Pluggable 1
OSC	Optical Supervisory Channel
OSM	OTN Switching Module
OTN	Optical Transport Network
PID	Password ID
POL	Pluggable Optical Layer
PWR	POWER

RAM	Random Access Memory
RNG	Random Number Generator
ROM	Read Only Memory
ROADM	Reconfigurable Optical Add-Drop Multiplexer
RSA	Rivest-Shamir-Adleman Public Key Algorithm
SAIM	Shelf Alarm Interface Module
SDM	Shelf Display Module
SD Card	Secure Digital Card
SEIM	Shelf Ethernet Interface Module
SFP	Small Form Pluggable
SFP+	Small Form Pluggable Plus
SHA	Secure Hash Algorithm
SPD	Security Policy Database
SNMP	Simple Network Management Protocol
SRAM	Static Random Access Memory
SSH	Secure Shell
STIM	Shelf Timing Interface Module
STPM	Shelf Timing and Processor Module
TL1	Transaction Language -1
TRNG	True Random Number Generator
UID	User Identifier
UTP	Universal Transport Platform

APPENDIX A Hardware procedures consistent with FIPS 140-2

Procedure 1: Install the mTera8 UTP FIPS kit

Purpose

The Infinera mTera8 UTP shelf requires the door and tamper-evident labels to be FIPS compliant.

Since the installation process for door has already been described with detailed information in [*mTera Install*], please refer to chapter 8 of installation manual [*mTera Install*]).

Procedure 2: Install the tamper-evident labels

Purpose

Use this procedure to provide to install the tamper-evident labels on an mTera8 UTP. Seal the systems only after you are sure that no additional provisioning/debugging is required. The tamper-evident label is shown in Figure 4.

Notes before tamper-evident labels installation

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

Steps

Note that the labels in the following steps refer to the tamper-evident label, label 1 is the small size label (2.363 inch 0.394 inch size), and label 2 and label 3 are the large size label (3.150 inch* 0.788 inch).*

1. Place label 1, label 2 and label 5 at the top right of the door shown as in figure 7 to protect the door from being opened.

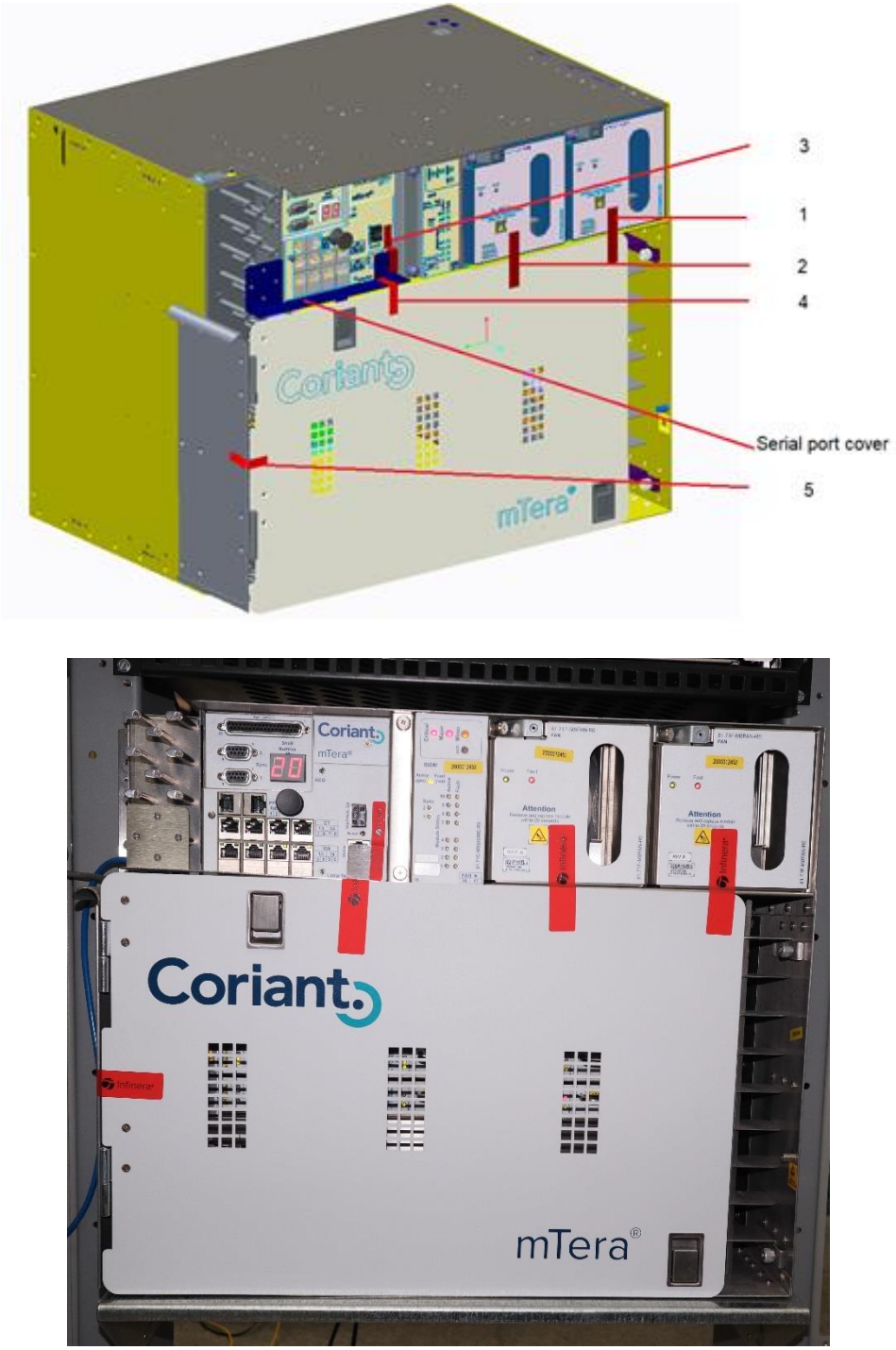

Figure 7 – Label placement at mTera8 UTP door

2. Place the "serial port cover" over the serial port of SIOM module to protect the shelf from being accessed through the serial port shown in figure 7. Install the four screws of the serial port cover as shown in Figure 8.

3. Place label 3 and label 4 over the “serial port cover” as shown in figure 7. Figure 8 shows the close-up view of serial port cover and label 3 & label 4.

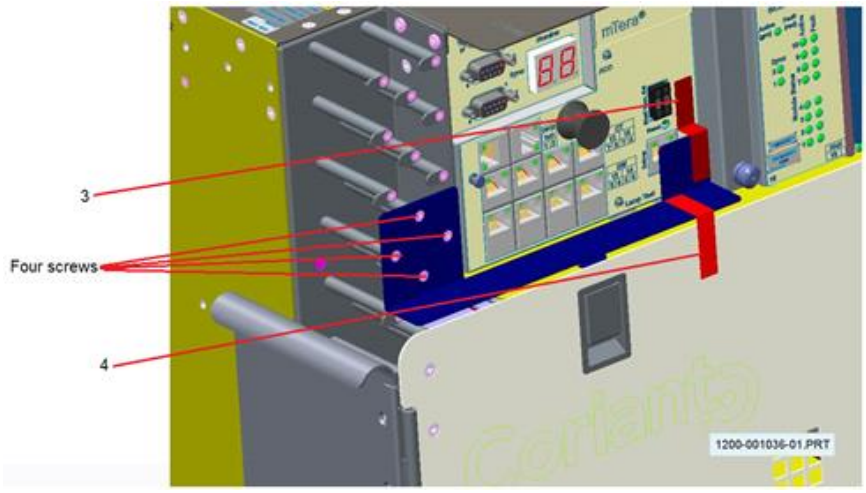

Figure 8 – Close-up view of serial port cover and label 3 & label 4