# FIPS 140-2 Non-Proprietary Security Policy

---

## Fujitsu Network Communications Inc.
## 1FINITY™ T600 Transport Blade

**Hardware version: T600**

**Firmware version: t600-19.1_cd42 and t600-19.1_cd188**

**Date: 12/11/2020**

Prepared by:

2400 Research Blvd, Suite 395
Rockville, MD 20850
tel: +1 (703) 375-9820
info@acumensecurity.net
www.acumensecurity.net

## Introduction

Federal Information Processing Standards Publication 140-2 — Security Requirements for Cryptographic Modules specifies requirements for cryptographic modules to be deployed in a Sensitive but Unclassified environment. The National Institute of Standards and Technology (NIST) and Canadian Centre for Cyber Security (CCCS) Cryptographic Module Validation Program (CMVP) run the FIPS 140 program. The NVLAP accredits independent testing labs to perform FIPS 140 testing; the CMVP validates modules meeting FIPS 140 validation. Validated is the term given to a module that is documented and tested against the FIPS 140 criteria.

More information is available on the CMVP website at:
https://csrc.nist.gov/projects/cryptographic-module-validation-program

## About this Document

This non-proprietary Cryptographic Module Security Policy for the Fujitsu Network Communications Inc. 1FINITY™ T600 Transport Blade provides an overview of the product and a high-level description of how it meets the overall Level 2 security requirements of FIPS 140-2.

The Fujitsu Network Communications Inc. 1FINITY™ T600 Transport Blade may also be referred to as the "module" in this document.

## Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. Fujitsu Network Communications Inc. shall have no liability for any error or damages of any kind resulting from the use of this document.

## Notices

# Table of Contents

# List of Tables



# List of Figures

# 1. Introduction

## 1.1 Scope

This document describes the cryptographic module security policy for the Fujitsu Network Communications Inc. 1FINITY™ T600 Transport Blade (Hardware version: T600) cryptographic module (also referred to as the "module" hereafter) with Firmware versions, t600-19.1_cd42 or t600-19.1_cd188. It contains specification of the security rules, under which the cryptographic module operates, including the security rules derived from the requirements of the FIPS 140-2 standard.

## 1.2 Overview

The 1FINITY™ T600 Transport Blade is a 1RU blade form factor programmable optical transponder supporting onboard software-provisioned data rates up to 600 Gbps over a single wavelength, using high-performance components and electronics. Powered by 3rd-generation digital signal processor (DSP) technology, the 1FINITY™ T600 Transport Blade delivers sophisticated and flexible modulation schemes and variable forward error correction (FEC). The advanced modulation flexibility provides optimum reach, capacity and power consumption, thereby enabling network operators to reduce cost per bit per kilometer for long-haul, metro ROADM or metro point-to-point applications.

For campus, regional, metro and long-haul data center interconnect (DCI) applications, the 1FINITY™ T600 Transport Blade enables data center and cloud operators to deploy flexible, cost-effective optical connections. The 1FINITY™ T600 Transport Blade helps operators meet the growing demands of the digital economy:

- Industry-leading capacity with 600 Gbps single-wavelength transmission
- Maximized optical performance and reach with programmable modes from 200 to 600 Gbps
- Highest spectral efficiency in the industry, achieving up to 76.8 Tbps per single fiber using C- and L-bands
- Cost-effective, energy-efficient power consumption of just 0.29 W per Gbps (fully-loaded)

In addition to its capacity and spectral efficiency, the 1FINITY™ T600 Transport Blade's superior rack-space density and low power consumption helps cut total cost of ownership in a variety of multihaul DCI applications. The 1FINITY™ T600 Transport Blade supports two transponder plug-in units and an integrated CPU complex, as well as redundant, replaceable fan modules and AC/DC power supply units. The plug-in units can each support a 1.2 TBps transponder with 12 QSFP28-based client ports mapped to two fixed network ports, achieving a total system density of 2.4 TBps per 1RU.

The following management protocols are supported by the 1FINITY™ T600 Transport Blade[1]:

- Access Control List (ACL) for user or system processes that granted access to objects and specify what operations are allowed on given objects.
- Command Line Interface (CLI) over a management interface or Telnet/Secure Shell (SSH) connection
- Dynamic Host Configuration Protocol (DHCP) Client used for obtaining configuration parameters

[1] Plaintext protocols shall not be used. Please see Section 10 in this document for instructions on the secure configuration and operation of the module.

- Domain Name System (DNS) Client used to help resolve DNS requests using external DNS server
- File Transfer Protocol/ Secure Transfer Protocol (FTP/SFTP) Server used for file transfer of system software, Log files, and Configuration files
- gRPC Network Management Interface (gNMI) used to install, manipulate, and delete the configuration of network devices, and to view operational data
- Link Layer Discovery Protocol (LLDP) used to advertise devices identity, capabilities and neighbors on a local area network
- Network Time Protocol (NTP) for network calendar timing
- Network Configuration Protocol (NETCONF) used to install, manipulate, and delete the configuration of network devices
- Open Shortest Path First (OSPF)
- Remote Authentication Dial-In User Service (RADIUS) protocol for centralized remote user authentication
- Remote Monitoring (RMON) for monitoring network operational activities
- Simple Network Management Protocol (SNMP) protocol with support for SNMPv1, SNMPv2c and SNMPv3 versions
- Streaming Telemetry enables access to real-time, model-driven, and analytics-ready data that can help with network automation, traffic optimization, and preventive troubleshooting on the module.
- Syslog protocol for monitoring device events by a remote server
- Terminal Access Controller Access-Control System Plus (TACACS+) protocol for centralized remote user authentication
- Zero Touch Provisioning (ZTP) used for provisioning the network infrastructure

# 2. Security Levels

The following table lists the level of validation for each area in FIPS 140-2:

| FIPS 140-2 Section Title | Validation Level |
|---|---|
| Cryptographic Module Specification | 2 |
| Cryptographic Module Ports and Interfaces | 2 |
| Roles, Services, and Authentication | 3 |
| Finite State Model | 2 |
| Physical Security | 2 |
| Operational Environment | N/A |
| Cryptographic Key Management | 2 |
| Electromagnetic Interference / Electromagnetic Compatibility | 2 |
| Self-Tests | 2 |
| Design Assurance | 3 |
| Mitigation of Other Attacks | N/A |
| Overall Level | 2 |

*Table 1 - Security Level*

# 3. Cryptographic Module Specification

## 3.1 Cryptographic Boundary

The cryptographic boundary is classified as a multi-chip standalone device and is the entire boundary of the chassis as pictured below.

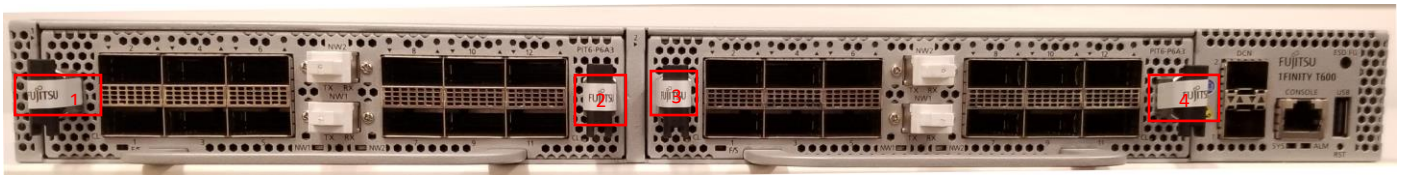


*Figure 1 – Front side of 1FINITY™ T600 Transport Blade*

*Figure 2 – Rear side of 1FINITY™ T600 Transport Blade*

*Figure 3 - Right side of 1FINITY™ T600 Transport Blade*

*Figure 4 - Left Side of 1FINITY™ T600 Transport Blade*

*Figure 5 - Top of 1FINITY™ T600 Transport Blade*

*Figure 6 - Bottom of 1FINITY™ T600 Transport Blade*

# 4. Cryptographic Module Ports and Interfaces

The module provides the following number of physical and logical interfaces to the device, and the physical interfaces provided by the module are mapped to the FIPS 140-2 defined logical interfaces: data input, data output, control input, status output, and power. The logical interfaces and their mapping are described in the following table:

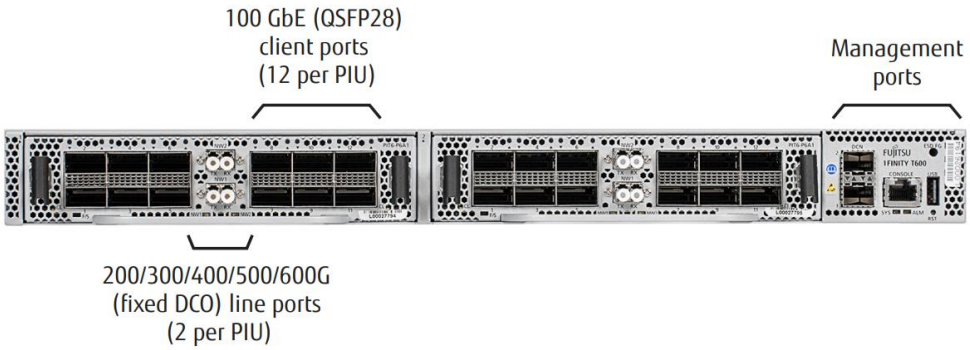


*Figure 7: 1FINITY™ T600 Transport Blade Ports*

| Physical Port | Qty. | FIPS 140-2 Logical Interface Mapping |
|---|---|---|
| RS232 RJ-45 **Console** Port | 1 | Control Input, Status Output |
| 100 Gbe (QSFP28) client ports | 24 (12 per PIU) | Data Input |
| 10BASE-T/100BASE-T/1000BASE-T/1000BASESX/1000BASE-LX10 Management ports | 2 | Data Input, Data Output, Control Input, Status Output |
| 200/300/400/500/600G (fixed DCO) line ports | 4 (2 per PIU) | Data Output |
| Dual replaceable AC or DC power supplies | 2 | Power |
| Replaceable Fans | 5 | N/A |
| Status LEDs | Total= 39<br>Data= 28<br>LX10 Mgmt(s)= 2<br>System= 1<br>ALARM= 1<br>F/S= 1<br>Power= 1<br>Fan= 5 | Status Output |

*Table 2 - Physical Port and Logical Interface Mapping*

# 5. Roles, Services and Authentication

## 5.1 Roles

The module supports eight different roles:

Read-only user, Performance Monitor Operator, Equipment Operator, Super User, System Operator, Security Operator, Crypto User and Crypto Officer (CO).

- Read-only user (Level-1): Read-only access privileges, can request alarm and PM information. *Level-1 cannot request security or encryption related information.

- Performance Monitor Operator (Level-2): Level-1 privileges plus can reset PM counters.

- Equipment Operator (Level-3): Level-2 privileges plus access to provision equipment and interfaces.

- Super User (Level-4): Full access to system, provisioning, security, and crypto encryption functions.

- System Operator (Level-5): Level-3 access privileges, plus access to system functions
    - Note: Level-5 cannot access security and crypto-encryption functions.
    - Note: Level-5 cannot add, change, or delete users.

- Security Operator (Level-6): Security access privileges only, can add, change, or delete users
    - Note: Level-6 cannot access system, provisioning, and crypto encryption functions.

- Crypto User (Level-7): Provision data-encryption interfaces and read the encryption status on the encryption-enabled interfaces.

- Crypto Officer (Level-8): Level-7 access privileges, plus can create crypto-user, crypto-officer, and can set global encryption policy.
    - Note: A Level-4 user must create the first Level 8 Crypto Officer account. Additional Level-8 user accounts can be created by a Level-4 or Level-8 user.

## 5.2 Services

The module provides the following Approved services which utilize algorithms listed in Table 8 and 9:

| Service | Super User (Level-4) | System Operator (Level-5) | Equipment Operator (Level-3) | Performance Monitor Operator (Level-2) | Read-only user (Level-1) | Security Operator (Level- 6) | Crypto User Role (Level-7) | Crypto Officer Role (Level-8) |
|---|---|---|---|---|---|---|---|---|
| Initialization | X | | | | | | | |
| Manage Other User Accounts | X | | | | | X | | X |
| Change Own Password | X | X | X | X | X | X | X | X |
| Provision Layer 1 Encryption | X | | | | | | X | X |
| Add/Change Pre-Shared Secret (DEK) | X | | | | | | X | X |
| Transfer Logs | X | | | | | | | X |
| System Provisioning | X | X | | | | | | |
| Equipment Provisioning | X | X | X | | | | | |
| Interface Provisioning | X | X | X | | | | | |
| View Equipment PM counters | X | X | X | X | X | | | |
| View Interface PM counters | X | X | X | X | X | | X | X |
| Clearing PM Counters | X | X | X | X | | | | |
| View Faults or Alarms | X | X | X | X | X | X | X | X |
| Request Status Information | X | X | X | X | X | | | |
| Export Backup of Configuration file over SFTP | X | X | | | | | | |
| View Network Element Configuration | X | X | X | X | X | | | |
| On-Demand Self-test | X | X | X | X | X | X | X | X |
| Zeroization/Factory Reset | X | X | | | | | | |
| Firmware Update | X | X | | | | | | |
| Set Configuration data | X | X | | | | | | |

*Table 3 - Approved Services and Role allocation*

The below table provides a full description of the unauthenticated services provided by the module:

| Unauthenticated Services |
|---|
| Request Authentication |
| On-Demand Self-test |

*Table 4 - Non-Approved Services*

The module provides the following non-Approved services which utilize algorithms listed in Table 12:

| Service |
|---|
| Non-Conformant Key Agreement |

*Table 5 - Non-Approved Services*

Services listed in Table 5 make use of non-compliant cryptographic algorithms. Use of these algorithms are prohibited in a FIPS-approved mode of operation.

## 5.3 Authentication

The module supports identity-based authentication. Operators must authenticate using a user ID and password or SSH client key (SSH only). The password entry feedback mechanism does not provide information that could be used to guess or determine the authentication data. Each User SSH session remains active (logged in) and secured until the operator logs out or inactivity for a configurable amount of time has elapsed. Each User Management Console session remains active until the operator logs out or inactivity for a configurable amount of time has elapsed.

| Type of Authentication | Authentication Strength |
|---|---|
| Operator Passwords | Passwords are required to be at least 8 characters in length and maximum of 128 characters (number of characters is dependent on the character set used by system). An 8-character password allowing all printable American Standard Code for Information Interchange (ASCII) characters (95) with repetition and a character restriction of: two uppercase characters, two lowercase characters, two numeric characters, two special characters equates to a 1: (26x26x26x26x10x10x33x33), or 1:49,764,686,400 chance of false acceptance.<br><br>The probability of a successful random attempt is 1: 49,764,686,400, which is less than 1/1,000,000.<br><br>The maximum number of possible attempts per minute is 3 (after 3 attempts operator is locked out for 1 minute). Therefore, the probability of a success with multiple consecutive attempts in a one-minute period is 3:49,764,686,400 which is less than the 1 in 100,000 required by FIPS 140-2. |
| Public keys | The module supports RSA based authentication of roles during SSH. Using conservative estimates and equating a 2048-bit RSA key to a 112-bit symmetric key, the probability for a random attempt to succeed is $1:2^{112}$ or 1: $5.19 \times 10^{33}$.<br><br>The probability of a successful random attempt is 1:2^112, which is less than 1/1,000,000.<br><br>Assuming the module can support 60 authentication attempts in one minute, the probability of a success with multiple consecutive attempts in a one-minute period is 60/2^112, which is less than the 1 in 100,000 required by FIPS 140-2. |
| SNMPv3<br><br>Authentication/ Privacy Password | Passwords are required to be at least 8 characters in length and maximum of 32 characters. An 8-character password allowing all printable American Standard Code for Information Interchange (ASCII) characters (95) with repetition equates to a 1: (95x95x95x95x95x95x95x95), or 1: 6,634,204,312,890,625 chance of false acceptance.<br><br>The probability of a successful random attempt is 1: 6,634,204,312,890,625, which is less than 1/1,000,000.<br><br>Assuming 10 attempts per second via a scripted or automatic attack, the probability of a success with multiple consecutive attempts in a one-minute period is 600/6,634,204,312,890,625, which is less than the 1 in 100,000 required by FIPS 140-2. |

*Table 6 - Authentication Types*

# 6. Physical Security

The module is a multi-chip standalone cryptographic module made with production grade components and standard passivation. The cover of the module is sealed with one circular tamper-evident seal[2] that covers a screw that needs to be removed to remove the cover of the module. The PIU's are sealed with four tamper-evident seals (2 per PIU), which are part of a FIPS kit and must be applied by the Crypto Officer on each PIU ear. The Crypto Officer must develop an inspection schedule to verify that the external enclosure of the modules and the tamper seals have not been damaged or tampered with in any way. The physical security of the module is intact if there is no evidence of tampering with the seals. If the Cryptographic Officer observes tamper evidence, it shall be assumed that the device has been compromised. The Cryptographic Officer shall retain control of the module and perform Zeroization of the module's CSPs by following the steps in Section 8.4 of the Security Policy and then follow the steps in Section 10 to place the module back into a FIPS-Approved mode of operation. The tamper-evident seals shall be installed for the module to operate in a FIPS Approved mode of operation.

The Crypto Officer is responsible for securing and having control at all times of any unused seals, and the direct control and observation of any changes to the module such as reconfigurations where the tamper evident seals or security appliances are removed or installed to ensure the security of the module is maintained during such changes and the module is returned to a FIPS approved state. The locations of the tamper-evident seals are indicated by the red rectangles in Figures 1 & 5[3].

Instructions for applying the tamper evident seals shall be followed and are as follows; the surfaces should be cleaned with 99% Isopropyl alcohol to remove dirt and oil before applying the seals. Handle the seals with care, do not touch the adhesive side of the seal and ensure the seal placement surface is completely clean and dry before applying the seals. If a seal needs to be re-applied, completely remove the old seal and follow the instructions for applying a new seal.

Additional seals can be requested through your Fujitsu sales contact. Reference the '246700000108A' SKU for Blade FIPS seals and '246700000115A' when ordering PIU FIPS seals.

# 7. Operational Environment

The module's operational environment is considered a limited operational environment under FIPS 140-2.

[2] This seal is applied by the manufacturer before shipment. During initial inspection of the module, if the end customer observes tamper evidence to this seal the module is DOA (Dead on Arrival) and the hardware is shipped back to FNC.

[3] Depicted on Page 7 & 8 of this document.

# 8. Cryptographic Algorithms and Key Management

## 8.1 Cryptographic Algorithms

The module implements the following approved algorithms in the firmware and hardware:

| Hardware Implementation Algorithms | | | | | |
|---|---|---|---|---|---|
| CAVP Cert # | Algorithm | Sizes | Standard | Mode/Method | Use |
| C1004 | AES | 256-bits | SP 800-38A<br>FIPS 197<br>SP 800-38D | ECB, GCM, CTR, GMAC | Encryption, Decryption |
| | KTS | 256-bits | IG D.9 | KTS (AES GCM) | Key Transport |

*Table 7 - Hardware Implementation Algorithms*

| Fujitsu Management Plane Cryptography Implementation | | | | | |
|---|---|---|---|---|---|
| CAVP Cert # | Algorithm | Sizes | Standard | Mode/Method | Use |
| C1319 | AES | 128, 192, 256-bits | SP 800-38A<br>SP 800-38B<br>SP 800-38C<br>SP 800-38D<br>SP 800-38E<br>FIPS 197 | CBC, ECB, CFB1, CFB8, CFB128, OFB, CCM, XTS[4], GCM, CTR, CMAC generation & verification | Encryption, Decryption, Authentication |
| C1319 | TDES | 168-bit | SP 800-67 | ECB, CBC, OFB, CFB1, CFB8, CFB64, CMAC generation & verification | Encryption, Decryption, Authentication |
| C1319 | KTS | 128, 192, 256-bits | IG D.9 | KTS (AES GCM) | Key Transport key establishment methodology provides between 128 and 256 bits of encryption strength |
| Vendor Affirmed | CKG | N/A | SP 800-133 | N/A | Key Generation |
| C1319 | CVL | P-224, P-256 P-384, P-521 | SP 800-56A | ECC CDH Component Testing | Key Agreement |
| C1319 | | Hash_DRBG & HMAC_DRBG: (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512) | SP 800-90Arev1 | Hash_DRBG, HMAC_DRBG, CTR_DRBG | Random Bit Generation |

[4] AES-XTS was CAVP tested (128-bit and 256-bit only) but is not used in any of the services implemented by the module in the Approved mode of operation.

| | | | | | |
|---|---|---|---|---|---|
| | DRBG | CTR_DRBG: (AES-128, AES-192, AES-256) | | | |
| C1319 | HMAC | 160, 224, 256, 384, 512-bits | FIPS PUB 198 | SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 | Message Authentication |
| C1319 | SHS | SHA-1, SHA-2 | FIPS PUB 180-4 | SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 | Message Digest Generation |
| C1319 | RSA | 2048, 3072 | FIPS PUB 186-2[5] & 186-4 | Key Generation9.31, Signature Generation9.31, Signature Verification9.31, Signature Generation PKCS1.5, Signature Verification PKCS1.5, Signature Generation PSS, Signature Verification PSS | Key Generation, Signature Generation, Signature Verification |
| C1319 | ECDSA | P-192[6], P-224, P-256 P-384, P-521 | FIPS PUB 186-4 | KeyGen, PKV, SigGen, SigVer | Key Generation, Signature Generation, Signature Verification |
| C1319 | DSA | 1024[7], 2048, 3072 | FIPS PUB 186-4 | KeyGen, PQGGen, PQGVer, SigGen, SigVer | Key Generation, Signature Generation, Signature Verification |
| C1319 | CVL | SHA-256, SHA-384 | SP 800-135 | TLS KDF (v1.0/1.1 and v1.2), SNMP KDF | Key Derivation |

*Table 8 - Fujitsu Management Plane Cryptography Implementation*

| Fujitsu Control Plane Cryptography Implementation | | | | | |
|---|---|---|---|---|---|
| CAVP Cert # | Algorithm | Sizes | Standard | Mode/Method | Use |
| C1317 | AES | 256-bits | FIPS 197 | ECB, CTR | Encryption, Decryption, Authentication |
| C1317 | SHS | SHA-2 | FIPS PUB 180-4 | SHA-384 | Message Digest Generation |
| C1317 | DRBG | AES-256 | SP 800-90Arev1 | CTR_DRBG | Random Bit Generation |

*Table 9 - Fujitsu Control Plane Cryptography Implementation*

| Fujitsu Management Plane SSH Implementation | | | | | |
|---|---|---|---|---|---|
| CAVP Cert # | Algorithm | Sizes | Standard | Mode/Method | Use |
| C1320 | CVL | SHA-1, SHA-256, SHA-512 | SP 800-135 | SSH KDF | Key Derivation |

*Table 10 - Fujitsu Management Plane SSH Implementation*

Note: Not all algorithms/modes tested on the CAVP validation certificates are implemented in the module.

[5] RSA SignGen (FIPS 186-2) is only approved for modulus 4096
[6] P-192 is only approved for ECDSA PKV and SigVer
[7] 1024 is only approved for DSA PQGVer and SigVer

### 8.1.1 Allowed Algorithms

The module implements the following allowed cryptographic algorithms:

| Algorithm | Use |
|---|---|
| NDRNG | To seed the Approved DRBG |
| Diffie-Hellman | Diffie-Hellman (CVL Certs. #C1319 and #C1320, key agreement; key establishment methodology provides 112 bits of encryption strength) |
| EC Diffie-Hellman | EC Diffie-Hellman (CVL Certs. #C1319 and #C1320, key agreement; key establishment methodology provides between 128 bits and 256 bits of encryption strength) |

*Table 11 - Allowed Algorithms*

No parts of the TLS, SNMP or SSH protocol, other than the KDF, have been tested by the CAVP and CMVP per FIPS 140-2 IG D.11.

Each of TLSv1.2 and SSHv2 protocols governs the generation of the respective Triple-DES keys. Refer to RFC 5246 (TLS) and RFC 4253 (SSH) for details relevant to the generation of the individual Triple-DES encryption keys. The user is responsible for ensuring the module limits the number of encryptions with the same key to 2^20.

### 8.1.2 Non-Approved Mode of Operation Non-Approved Algorithms and Protocols with No Security Claimed

The module supports the following non-Approved but allowed algorithms with no security claimed:

- AES encryption/decryption used to obfuscate files stored on the module.

The operator shall consult FIPS 140-2 IG 1.23 for further understanding of the use of functions where no security is claimed.

### 8.1.3 Non-Approved Mode of Operation

The Crypto Officer is responsible for configuration of the module. When configured according to the Section 10 in this Security Policy, the module only supports the non-Approved service listed in Table 5. The non-Approved algorithms or plaintext protocols in Section 10 are disabled.

### 8.1.4 Non-Approved Algorithms

The module implements the following algorithms which are considered non-Approved:

| Algorithm | |
|---|---|
| Diffie-Hellman | Less than 112 bits of encryption strength. |
| RSA | Less than 112 bits of encryption strength. |

*Table 12 - Non-Approved Algorithms*

## 8.2 Cryptographic Key Management

The module supports the following CSPs listed below in Table 10:

| Keys and CSPs | Description | Key/CSP Type | Generation /Input | Output Method | Storage | Zeroization |
|---|---|---|---|---|---|---|
| Operator Passwords | Authentication for Read-only User, Performance Monitor | Minimum of 8 (64 bits) and maximum of 128 bytes (1024 bits) string | Externally generated. Enters the module in encrypted form via | Exits encapsulated (SSH/SFTP) in configuration backup | Hashed in non-volatile Flash | Invoke Factory Reset or Zeroization command |

| Keys and CSPs | Description | Key/CSP Type | Generation /Input | Output Method | Storage | Zeroization |
|---|---|---|---|---|---|---|
| | Operator, Equipment Operator, Super User, System Operator, Security Operator, Crypto User, Crypto Officer (level-1 to level-8 users) | value | a secure TLS or SSH/SFTP session.<br><br>Enters the module in plaintext via a directly attached cable to the serial port | | memory | |
| EC DH Key Pair for DEK | Key pair used in NIST SP 800-56A (Section 5.7.1.2) ECC CDH Primitive computation | EC DH private component 384-bits<br><br>EC DH public key (P-384) | Generated internally using the SP 800-90A CTR_DRBG<br>Public key of a peer enters the module in plaintext | Private never exits the module | Plaintext in volatile memory | Session termination or power cycle or key rotation |
| ECC CDH primitive for DEK | Shared Secret (Z) value that will be used to derive the DEK | 384-bit string | Computed per SP 800-56Arev1 (Section 5.7.1.2) | Never exits the module | Plaintext in volatile memory | Session termination or power cycle or key rotation |
| Data Encryption Key (DEK) | Used for encrypting or decrypting payload data | AES-GCM 256 bit | Derived per NIST SP 800-56A (Section 5.8.1) | Never exits the module | Plaintext in volatile memory | Power Cycle or key rotation |
| Peer-Authentication Pre-Shared Secret | Entered by Super User, Crypto User, Crypto Officer (level-4, 7 or 8). Parameter used for Peer-Authentication during key exchange | 384-bit string | Externally generated. Enters the module in encrypted form via SSH, TLS or Console (users enter in plain-text but encrypted through transport protocol) | Exits encapsulated (SSH or TLS) in configuration backup | Encrypted in non-volatile Flash memory | Invoke Factory Reset or Zeroization command |
| Diffie-Hellman (DH) Key Pair | Negotiating TLS or SSH/SFTP sessions | Diffie-Hellman private component 160 – 512 bits<br><br>Public component 2048 bits | Generated internally using the SP 800-90A CTR_DRBG<br><br>Public key of a peer enters the module in plaintext | Private never exits the module | Plaintext in volatile memory | Session termination or power cycle |
| Elliptic Curve | Negotiating TLS | EC DH private | Generated | Private never | Plaintext in | Session |

| Keys and CSPs | Description | Key/CSP Type | Generation /Input | Output Method | Storage | Zeroization |
|---|---|---|---|---|---|---|
| Diffie-Hellman (ECDH) Key Pair | or SSH/SFTP sessions | component 384-bits<br><br>EC DH public key (P-256, P-384 and P-521) | internally using the SP 800-90A CTR_DRBG<br><br>Public key of a peer enters the module in plaintext | exits the module | volatile memory | termination or power cycle |
| SNMP Privacy Key | Encryption / decryption of SNMP session traffic | AES CFB 128 bit | Derived using SP 800-135 Key derivation (SNMP) | Exits encapsulated (SSH/SFTP) in configuration backup | Plaintext in non-volatile Flash memory | Invoke Factory Reset or Zeroization command |
| SNMP Authentication Key | Message authentication and verification in SNMP | HMAC-SHA-1 | Derived using SP 800-135 Key derivation (SNMP) | Exits encapsulated (SSH/SFTP) in configuration backup | Plaintext in non-volatile Flash memory | Invoke Factory Reset or Zeroization command |
| SNMPv3 Authentication / Privacy Password | Password | Minimum of 8 (64 bits) and maximum of 32 bytes (160 bits) string value | Externally generated. Enters the module in encrypted form via a secure TLS or SSH session. | Exits encapsulated (SSH/SFTP) in configuration backup | Plaintext in non-volatile Flash memory | Invoke Factory Reset or Zeroization command |
| SSH/SFTP Host Key Pair | Key Pair used for SSH/SFTP authentication | RSA 2048-bit | Internally generated via FIPS-Approved DRBG upon first system power-up | Private never exits the module | Plaintext in non-volatile Flash memory | Zeroization command |
| TLS Premaster Secret | Establish the TLS Master Secret | 384-bit string | Generated internally with the SP 800-90A CTR_DRBG<br><br>Input during TLS negotiation | Exits in encrypted form during protocol handshake | Plaintext in volatile memory | Session termination or power cycle |
| TLS Master Secret | Establish the TLS Session Key | 384-bit string | Derived [8]from the TLS Pre-Master Secret | Never exits the module | Plaintext in volatile memory | Session termination or power cycle |
| TLS Session Key | Used for encrypting/ decrypting TLS messages | AES CBC or GCM 128 or 256-bit key, 168-bit Triple-DES ECBC | Generated internally during session negotiation | Exits in encrypted form during protocol handshake | Plaintext in volatile memory | Session termination or power cycle |

[8] Derived via NIST SP 800-135 TLS 1.2 KDF

| Keys and CSPs | Description | Key/CSP Type | Generation /Input | Output Method | Storage | Zeroization |
|---|---|---|---|---|---|---|
| TLS Authentication Key | Used for authenticating TLS messages | HMAC SHA-1-, 256-, 384-bit key | Generated internally during session negotiation | Never exits the module | Plaintext in volatile memory | Session termination or power cycle |
| SSH/SFTP Session Encryption Key | Used for Encrypting SSH/SFTP messages | AES CBC or CTR 128-, 192, or 256-bit key/ GCM 128-or 256-bit/ 168-bit Triple-DES ECBC | Internally generated via FIPS-Approved DRBG | Exits in encrypted form during protocol handshake | Plaintext in volatile memory | Session termination or power cycle |
| SSH/SFTP Session Authentication Key | Data authentication for SSH/SFTP sessions | HMAC SHA-1-, 96, 256-, or 512-bit key | Derived via in SP800-135 KDF (SSH) | Never exits the module | Plaintext in volatile memory | Session termination or power cycle |
| SP 800-90A CTR_DRBG Seed | Seeding material for the SP800-90A CTR_DRBG | 384-bit value | Internally generated by the NDRNG | Never exits the module | Plaintext in volatile memory | Power cycle |
| SP 800-90A CTR_DRBG Nonce | Entropy material for the SP800-90A CTR_DRBG | 128-bit value | Internally generated by the NDRNG | Never exits the module | Plaintext in volatile memory | Power cycle |
| SP 800-90A CTR_DRBG key value | Used for the SP 800-90A CTR_DRBG | Internal state value | Internally generated | Never exits the module | Plaintext in volatile memory | Power cycle |
| SP 800-90A CTR_DRBG V value | Used for the SP 800-90A CTR_DRBG | Internal state value | Internally generated | Never exits the module | Plaintext in volatile memory | Power cycle |

*Table 13 - Approved Keys and CSPs Table*

The module implements the following access control policy on keys and CSPs in the module shown in the following table. The Access Policy is noted by R=Read, W=Write and X=Execute.

| Service | CSP Access | Right (R/W/X) |
|---|---|---|
| Initialization | Diffie-Hellman (DH) Key Pair, Elliptic Curve Diffie-Hellman (ECDH) Key Pair, TLS Premaster Secret, TLS Master Secret, TLS Session Key, TLS Authentication Key, SSH/SFTP Host Key Pair, SSH/SFTP Session Encryption Key, SSH/SFTP Session Authentication Key, SP 800-90A CTR_DRBG Seed, SP 800-90A CTR_DRBG Nonce, SP 800-90A CTR_DRBG key value, SP 800-90A V value | R/W/X |
| Manage Other User Accounts | Operator Passwords , Diffie-Hellman (DH) Key Pair, Elliptic Curve Diffie-Hellman (ECDH) Key Pair, TLS Premaster Secret, TLS Master Secret, TLS Session Key, TLS Authentication Key; SSH/SFTP Host Key Pair, SSH/SFTP Session Encryption Key, SSH/SFTP Session Authentication key, SP 800-90A CTR_DRBG | R/W/X |

| | | |
|---|---|---|
| | Seed, SP 800-90A CTR_DRBG Nonce, SP 800-90A CTR_DRBG key value, SP 800-90A V value | |
| Change Own Password | Operator Password, Diffie-Hellman (DH) Key Pair, Elliptic Curve Diffie-Hellman (ECDH) Key Pair, TLS Premaster Secret, TLS Master Secret, TLS Session Key, TLS Authentication Key; SSH/SFTP Host Key Pair, SSH/SFTP Session Encryption Key, SSH/SFTP Session Authentication key, SP 800-90A CTR_DRBG Seed, SP 800-90A CTR_DRBG Nonce, SP 800-90A CTR_DRBG key value, SP 800-90A V value | R/W/X |
| Provision Layer 1 Encryption | Operator Password | R |
| | EC DH Key Pair for DEK, ECC CDH primitive for DEK, DEK, Peer-Authentication Pre-Shared Secret, Diffie-Hellman (DH) Key Pair, Elliptic Curve Diffie-Hellman (ECDH) Key Pair, TLS Premaster Secret, TLS Master Secret, TLS Session Key, TLS Authentication Key; SSH/SFTP Host Key Pair, SSH/SFTP Session Encryption Key, SSH/SFTP Session Authentication key, SP 800-90A CTR_DRBG Seed, SP 800-90A CTR_DRBG Nonce, SP 800-90A CTR_DRBG key value, SP 800-90A V value | R/W/X |
| Add/Change Pre-Shared Secret (DEK) | Operator Password | R |
| | EC DH Key Pair for DEK, ECC CDH primitive for DEK, DEK, Peer-Authentication Pre-Shared Secret, Diffie-Hellman (DH) Key Pair, Elliptic Curve Diffie-Hellman (ECDH) Key Pair, TLS Premaster Secret, TLS Master Secret, TLS Session Key, TLS Authentication Key; SSH/SFTP Host Key Pair, SSH/SFTP Session Encryption Key, SSH/SFTP Session Authentication key, SP 800-90A CTR_DRBG Seed, SP 800-90A CTR_DRBG Nonce, SP 800-90A CTR_DRBG key value, SP 800-90A V value | R/W/X |
| Transfer Encryption Logs | Operator Password | R |
| | Diffie-Hellman (DH) Key Pair, Elliptic Curve Diffie-Hellman (ECDH) Key Pair, TLS Premaster Secret, TLS Master Secret, TLS Session Key, TLS Authentication Key, SSH/SFTP Host Key Pair, SSH/SFTP Session Encryption Key, SSH/SFTP Session Authentication Key, SP 800-90A CTR_DRBG Seed, SP 800-90A CTR_DRBG Nonce, SP 800-90A CTR_DRBG key value, SP 800-90A V value | R/W/X |
| System Provisioning | Operator Password | R |
| | SNMP Privacy Key, SNMP Authentication Key, SNMPv3 Authentication/ Privacy Password; DH Key Pair, ECDH Key Pair, TLS Premaster Secret, TLS Master Secret, TLS Session Key, TLS Authentication Key; SSH/SFTP Host Key Pair, SSH/SFTP Session Encryption Key, SSH/SFTP Session Authentication key, SP 800-90A CTR_DRBG Seed, SP 800-90A CTR_DRBG Nonce, SP 800-90A CTR_DRBG key value, SP 800-90A V value | R/W/X |
| Equipment Provisioning | Operator Password | R |

| | | |
|---|---|---|
| | Diffie-Hellman (DH) Key Pair, Elliptic Curve Diffie-Hellman (ECDH) Key Pair, TLS Premaster Secret, TLS Master Secret, TLS Session Key, TLS Authentication Key; SSH/SFTP Host Key Pair, SSH/SFTP Session Encryption Key, SSH/SFTP Session Authentication key, SP 800-90A CTR_DRBG Seed, SP 800-90A CTR_DRBG Nonce, SP 800-90A CTR_DRBG key value, SP 800-90A V value | R/W/X |
| Interface Provisioning | Operator Password | R |
| | Diffie-Hellman (DH) Key Pair, Elliptic Curve Diffie-Hellman (ECDH) Key Pair, TLS Premaster Secret, TLS Master Secret, TLS Session Key, TLS Authentication Key; SSH/SFTP Host Key Pair, SSH/SFTP Session Encryption Key, SSH/SFTP Session Authentication key, SP 800-90A CTR_DRBG Seed, SP 800-90A CTR_DRBG Nonce, SP 800-90A CTR_DRBG key value, SP 800-90A V value | R/W/X |
| View Equipment PM counters | Operator Password | R |
| | Diffie-Hellman (DH) Key Pair, Elliptic Curve Diffie-Hellman (ECDH) Key Pair, TLS Premaster Secret, TLS Master Secret, TLS Session Key, TLS Authentication Key; SSH/SFTP Host Key Pair, SSH/SFTP Session Encryption Key, SSH/SFTP Session Authentication key, SP 800-90A CTR_DRBG Seed, SP 800-90A CTR_DRBG Nonce, SP 800-90A CTR_DRBG key value, SP 800-90A V value | R/W/X |
| View Interface PM counters | Operator Password | R |
| | Diffie-Hellman (DH) Key Pair, Elliptic Curve Diffie-Hellman (ECDH) Key Pair, TLS Premaster Secret, TLS Master Secret, TLS Session Key, TLS Authentication Key; SSH/SFTP Host Key Pair, SSH/SFTP Session Encryption Key, SSH/SFTP Session Authentication key, SP 800-90A CTR_DRBG Seed, SP 800-90A CTR_DRBG Nonce, SP 800-90A CTR_DRBG key value, SP 800-90A V value | R/W/X |
| Clear PM Counters | Operator Password | R |
| | Diffie-Hellman (DH) Key Pair, Elliptic Curve Diffie-Hellman (ECDH) Key Pair, TLS Premaster Secret, TLS Master Secret, TLS Session Key, TLS Authentication Key; SSH/SFTP Host Key Pair, SSH/SFTP Session Encryption Key, SSH/SFTP Session Authentication key, SP 800-90A CTR_DRBG Seed, SP 800-90A CTR_DRBG Nonce, SP 800-90A CTR_DRBG key value, SP 800-90A V value | R/W/X |
| View Faults or Alarms | Operator Password | R |
| | Diffie-Hellman (DH) Key Pair, Elliptic Curve Diffie-Hellman (ECDH) Key Pair, TLS Premaster Secret, TLS Master Secret, TLS Session Key, TLS Authentication Key; SSH/SFTP Host Key Pair, SSH/SFTP Session Encryption Key, SSH/SFTP Session Authentication key, SP 800-90A CTR_DRBG Seed, SP 800-90A CTR_DRBG Nonce, SP 800-90A CTR_DRBG key value, SP 800-90A V value | R/W/X |
| Request Status Information | Operator Password | R |
| | Diffie-Hellman (DH) Key Pair, Elliptic Curve Diffie-Hellman (ECDH) Key Pair, TLS Premaster Secret, TLS Master Secret, TLS | R/W/X |

| | | |
|---|---|---|
| | Session Key, TLS Authentication Key; SSH/SFTP Host Key Pair, SSH/SFTP Session Encryption Key, SSH/SFTP Session Authentication key, SP 800-90A CTR_DRBG Seed, SP 800-90A CTR_DRBG Nonce, SP 800-90A CTR_DRBG key value, SP 800-90A V value | |
| Export Backup of Configuration file over SFTP | Operator Password | R |
| | Diffie-Hellman (DH) Key Pair, Elliptic Curve Diffie-Hellman (ECDH) Key Pair, TLS Premaster Secret, TLS Master Secret, TLS Session Key, TLS Authentication Key; SSH/SFTP Host Key Pair, SSH/SFTP Session Encryption Key, SSH/SFTP Session Authentication key, SP 800-90A CTR_DRBG Seed, SP 800-90A CTR_DRBG Nonce, SP 800-90A CTR_DRBG key value, SP 800-90A V value | R/W/X |
| View Network Element Configuration | Operator Password | R |
| | Diffie-Hellman (DH) Key Pair, Elliptic Curve Diffie-Hellman (ECDH) Key Pair, TLS Premaster Secret, TLS Master Secret, TLS Session Key, TLS Authentication Key; SSH/SFTP Host Key Pair, SSH/SFTP Session Encryption Key, SSH/SFTP Session Authentication key, SP 800-90A CTR_DRBG Seed, SP 800-90A CTR_DRBG Nonce, SP 800-90A CTR_DRBG key value, SP 800-90A V value | R/W/X |
| On-Demand Self-test | N/A | N/A |
| Zeroization/Factory Reset | All CSP's | R/W/X |
| Firmware Update | Operator Password | R |
| | Diffie-Hellman (DH) Key Pair, Elliptic Curve Diffie-Hellman (ECDH) Key Pair, TLS Premaster Secret, TLS Master Secret, TLS Session Key, TLS Authentication Key; SSH/SFTP Host Key Pair, SSH/SFTP Session Encryption Key, SSH/SFTP Session Authentication key, SP 800-90A CTR_DRBG Seed, SP 800-90A CTR_DRBG Nonce, SP 800-90A CTR_DRBG key value, SP 800-90A V value | R/W/X |
| Set Configuration data | Operator Password | R |
| | Diffie-Hellman (DH) Key Pair, Elliptic Curve Diffie-Hellman (ECDH) Key Pair, TLS Premaster Secret, TLS Master Secret, TLS Session Key, TLS Authentication Key; SSH/SFTP Host Key Pair, SSH/SFTP Session Encryption Key, SSH/SFTP Session Authentication key, SP 800-90A CTR_DRBG Seed, SP 800-90A CTR_DRBG Nonce, SP 800-90A CTR_DRBG key value, SP 800-90A V value | R/W/X |

*Table 14 - Approved Service to Key/CSP Mapping*

## 8.3 Key Generation and Entropy

The module's primary entropy source is an entropy-generating NDRNG inside the module's cryptographic boundary consistent with Scenario 1 (a) described in FIPS 140-2 IG 7.14. The module performs a CRNGT on the entropy input it receives. The Approved CTR_DRBGs in the Fujitsu Management Plane Cryptography Implementation library and Fujitsu Control Plane Cryptography Implementation library will each request 384-bits from the Linux output pools when needed.

Seed created by NDRNG and used to seed the CTR_DRBG. The Nonce is 128 bits and the Entropy input is 256 bits for a total seed size of 384 bits.

In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation (CKG) as per SP 800-133 (vendor affirmed). The resulting generated symmetric keys are the unmodified output from the SP 800-90A DRBG.

### 8.4 Zeroization

Ephemeral secret keys are zeroized either at session termination or by power-cycling the module. Persistently stored CSPs can also be zeroized by issuing a factory reset command, "request zeroize-system". This changes all values back to zero or the default values. Targeted Zeroization of CSPs used for L1 data encryption can also completed by issuing the "request zeroize-data-encryption" command.

If the module transitions from the non-Approved to the Approved mode or vice versa, the module shall be zeroized prior to switching modes.

The output data path is provided by the data interfaces and is logically disconnected from processes performing key generation or zeroization. No key information will be output through the data output interface when the module zeroizes keys.

## 9. Self-tests

FIPS 140-2 requires the module to perform self-tests to ensure the module integrity and the correctness of the cryptographic functionality at start-up. Some functions require conditional tests during normal operation of the module.

### 9.1 Power-On Self-Tests

Power-on self-tests are run upon the initialization of the module and do not require operator intervention to run. If any of the tests fail, the module will return an error code and transition to an error state where no functions can be executed. An operator can attempt to reset the state by cycling the power. However, the failure of a self-test may require the module to be replaced.

The module implements the following power-on self-tests in the Module:

| Type | Test Description |
|---|---|
| Integrity Test | • File Integrity (CRC-32)<br>• Blade FPGA FW Integrity (CRC-32)<br>• DCO FW Integrity (CRC-16)<br>• DSP FW Integrity (CRC-16) |
| Known Answer Tests | • Hardware AES ECB KAT (Encryption and Decryption. Size 256)<br>• Hardware AES GCM KAT (Encryption and Decryption. Size 256)<br>• Fujitsu Management Plane Cryptography<br>  ○ Firmware AES CBC KAT (Encryption and Decryption. Size 128,192,256)<br>  ○ Firmware AES GCM KAT (Encryption and Decryption. Size 128, 256)<br>  ○ Firmware TDES CBC KAT (Encryption and Decryption)<br>  ○ Firmware SHS KAT (SHA-1, SHA-256 and SHA-512)<br>  ○ Firmware HMAC KAT (HMAC-SHA-1, -SHA-256, -SHA-384, -SHA-512)<br>  ○ Firmware SP 800-90A CTR_DRBG KAT<br>  ○ Firmware RSA KAT (Sign and Verify. Size 2048)<br>  ○ Firmware DSA KAT (Sign and Verify Size 2048)<br>  ○ Firmware ECDSA KAT (Sign and Verify. Size P-256) |

| | |
|---|---|
| | ○ Firmware EC Diffie-Hellman Primitive “Z” Computation KAT<br>• Fujitsu Control Plane Cryptography<br>○ Firmware AES ECB KAT (Encryption and Decryption. Size 256)<br>○ Firmware ECDHE KAT<br>○ Firmware SP 800-90A CTR_DRBG KAT<br>○ Firmware SHS KAT (SHA-384) |

*Table 15 - Power-up Self-tests*

The module performs all power-on self-tests automatically when it is initialized. All power-on self-tests must be passed before a User/Crypto Officer can perform services. The Power-on self-tests can be run on demand by rebooting the module in FIPS approved Mode of Operation. Should any of the above tests fails, the device enters an error state. In an error state no traffic is allowed in or out of the device on the ethernet ports.

### 9.2 Conditional Self-Tests

Conditional self-tests are test that run during operation of the module. Each module performs the following conditional self-tests:

| Type | Test Description |
|---|---|
| CRNGT on NDRNG | Continuous RNG test (CRNGT) performed on entropy input from the TRNG |
| CRNGT on the DRBG | Continuous RNG test (CRNGT) for the SP800-90A DRBG |
| Pairwise Consistency Test | RSA/ ECDSA Key Generation |
| Firmware Load Test | RSA based integrity test to verify firmware to be loaded into the module |

*Table 16 - Conditional Self-tests*

### 9.3 Critical Function Tests

The module implements the following critical function tests which execute at start-up or during operation of the module.

| Type | Test Description |
|---|---|
| DRBG Health Tests | Performed on DRBG, per SP 800-90A Section 11.3. Required per IG W.3. |

*Table 17 – Critical Function Tests*

## 10. Guidance and Secure Operation

This section describes the configuration, maintenance, and administration of the cryptographic module. The Crypto Officer is responsible for ensuring none of the plaintext protocols are used and non-Approved ciphers in Section 10 are disabled. When configured according to the Section 10 in this Security Policy, the module only runs in the FIPS-Approved mode of operation with the exception of the Services in Table 5. Services listed in Table 5 make use of non-compliant cryptographic algorithms. Use of these algorithms are prohibited in a FIPS-approved mode of operation.

When the module is powered on, its power-up self-tests are executed without any operator intervention.

## 10.1 Initialization

The operator shall set up the device as defined in the Fujitsu 1FINITY™ T600 Transport Blade Security Guide. The Crypto-Officer shall also:

- Verify that the firmware version of the module is t600-19.1_cd42 or t600-19.1_cd188.
- Ensure the default password of the Super User and Crypto Officer is changed upon first use.
- All operator passwords must be a minimum of 8 characters in length meeting the following character restrictions;
    - two uppercase characters
    - two lowercase characters
    - two numeric characters
    - two special characters
- The following should be disabled prior to enabling FIPS and shall not be used in the FIPS Approved mode of operation;
    - RADIUS
    - TACACS+
    - ZTP
    - USB
    - Root Access
    - Telnet
    - FTP
    - HTTP
    - Bypass encryption
    - SNMP-v1/v2c
- Console shall be enabled.
- SNMPv3 to allow only secure auth/priv methods
- Password mode should be fips-compatible.
- ciphers should be fips-compatible.
- ssh-algorithm should be fips-compatible
- For SSH/SFTP, ensure modulus sizes of 2048-bits of strength or use group 14 selected for Diffie-Hellman.
- Ensure that SSH is configured to use RSA for authentication.
- Ensure RSA keys are at least 2048-bit keys. No 512-bit or 1024-bit keys shall be used in FIPS mode of operation.

The system shall be considered to be in the non-approved mode of operation if any of the non-compliant algorithms listed in Section 8.1.3 are used.

## 10.2 Usage of AES GCM in the module

The module's software AES-GCM implementation conforms to IG A.5 scenario #1 following RFC 5288 for TLS. The module is compatible with TLS v1.2 and provides support for the acceptable GCM cipher suites from SP 800-52 Rev1, Section 3.3.1. 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 case the module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption shall be established.

For SSH, the IV conforms to the SSHv2 specification and is compliant with RFCs 4252, 4253 and RFC 5647 and FIPS 140-2 IG A.5 scenario #1.

The module's hardware AES-GCM implementation conforms to IG A.5, scenario #3. The module uses deterministic construction where the 96-bit IV is the concatenation of two fields, the fixed field and the invocation field. The fixed field is the 32-bit Device Field (Engine #ID) and the invocation field is the 64-bit counter. The block counter in the IV is incremented every OTN frame. The module forces a counter reset/new IV every 48 hours for the core. If a new key is not derived before the maximum limit, the module raises a flag/alarm.

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 $2^{-32}$.

The module enforces FIPS 140-2 IG A.5, which states that in case the module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption shall be established.

# 11. Glossary

| Term | Description |
|---|---|
| AES | Advanced Encryption Standard |
| CAVP | Cryptographic Algorithm Validation Program |
| CFB | Cipher Feedback |
| CKG | Cryptographic Key Generation |
| CMVP | Cryptographic Module Validation Program |
| CRNGT | Continuous Random Number Generator Test |
| CSP | Critical Security Parameter |
| CTR | Counter |
| DCO | Digital Controlled Oscillator |
| DRBG | Deterministic Random Bit Generator |
| DSP | Digital Signal Processor |
| ECB | Electronic Codebook |
| FIPS | Federal Information Processing Standards |
| GCM | Galois/Counter Mode |
| IG | Implementation Guidance |
| IV | Initialization vector |
| KAT | Known answer test |
| KDF | Key-Derivation Function |
| NIST | National Institute of Standards and Technology |
| NDRNG | Non-Deterministic Random Number Generator |
| OTN | Optical Transport Network |
| QSFP | Quad Small Form-factor Pluggable |
| RSA | Rivest Shamir Adleman |
| SHA | Secure Hash Algorithm |
| SHS | Secure Hash Standard |
| TBps | Terabytes per second |
| TRNG | True Random Number Generator |

*Table 18 - Glossary of Terms*