

ECI Telecom Ltd / Ribbon communications Operating company, Inc.

TM400ENB

FIPS 140-3 Non-Proprietary Security Policy

Document Version 1.4
September 2026

Prepared by:



www.jtsec.es

Table of Contents

1 General 4
1.1 Overview 4
1.2 Security Levels 4
1.3 Additional Information 4
2 Cryptographic Module Specification 5
2.1 Description 5
2.2 Tested and Vendor Affirmed Module Version and Identification 7
2.3 Excluded Components 8
2.4 Modes of Operation 9
2.5 Algorithms 9
2.6 Security Function Implementations 11
2.7 Algorithm Specific Information 15
2.8 RBG and Entropy 15
2.9 Key Generation 16
2.10 Key Establishment 17
2.11 Industry Protocols 17
3 Cryptographic Module Interfaces 18
3.1 Ports and Interfaces 18
4 Roles, Services, and Authentication 22
4.1 Authentication Methods 22
4.2 Roles 23
4.3 Approved Services 24
4.4 Non-Approved Services 34
4.5 External Software/Firmware Loaded 34
4.6 Bypass Actions and Status 34
5 Software/Firmware Security 36
5.1 Integrity Techniques 36
5.2 Initiate on Demand 36
6 Operational Environment 37
6.1 Operational Environment Type and Requirements 37
7 Physical Security 38
7.1 Mechanisms and Actions Required 38
7.2 EFP/EFT Information 41
7.3 Hardness Testing Temperature Ranges 41

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

8 Non-Invasive Security 42
9 Sensitive Security Parameters Management 43
9.1 Storage Areas 43
9.2 SSP Input-Output Methods 43
9.3 SSP Zeroization Methods 45
9.4 SSPs 46
9.5 Transitions 51
10 Self-Tests 52
10.1 Pre-Operational Self-Tests 52
10.2 Conditional Self-Tests 55
10.3 Periodic Self-Test Information 64
10.4 Error States 67
10.5 Operator Initiation of Self-Tests 68
11 Life-Cycle Assurance 69
11.1 Installation, Initialization, and Startup Procedures 69
11.2 Administrator Guidance 70
11.3 Non-Administrator Guidance 70
11.4 Design and Rules 70
11.5 End of Life 71
12 Mitigation of Other Attacks 75

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

List of Tables

Table 1: Security Levels 4
Table 2: Tested Module Identification – Hardware 8
Table 3: Modes List and Description 9
Table 4: Approved Algorithms 10
Table 5: Vendor-Affirmed Algorithms 11
Table 6: Security Function Implementations 15
Table 7: Entropy Certificates 16
Table 8: Entropy Sources 16
Table 9: Ports and Interfaces 20
Table 10: Client & Line ports assignment 20
Table 11: Authentication Methods 23
Table 12: Roles 23
Table 13: Approved Services 34
Table 14: Mechanisms and Actions Required 38
Table 15: EFP/EFT Information 41
Table 16: Hardness Testing Temperatures 41
Table 17: Storage Areas 43
Table 18: SSP Input-Output Methods 45
Table 19: SSP Zeroization Methods 46
Table 20: SSP Table 1 49
Table 21: SSP Table 2 51
Table 22: Pre-Operational Self-Tests 53
Table 23: Conditional Self-Tests 62
Table 24: Pre-Operational Periodic Information 65
Table 25: Conditional Periodic Information 67
Table 26: Error States 68

List of Figures

Figure 1: Ribbon Communications TM400ENB Module (Top View) 5
Figure 2: Ribbon Communications TM400ENB Module (Bottom View) 6
Figure 3: System Level Overview. Block Diagram 6
Figure 4: Ribbon Communications TM400ENB Board Assembly 9
Figure 5: Random Number Generator 16
Figure 6: Ports and interfaces on TM400ENB in front and back sides 18
Figure 7: Tamper Evidence Seals Applied Across Critical Areas of the module 40
Figure 8: Metallic Tamper Shield Sealed and Mated with the PCB (front) 40
Figure 9: Front Panel Before Installing Pick Resistant Lock 41

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

1 General

1.1 Overview

This document is the FIPS 140-3 non-proprietary security policy for Ribbon Communications Encryption Module TM400ENB (hardware version D.1 and firmware version (V13.5.1.0.+) which will also be referred to as "the module" through this document. Ribbon Communications Encryption Module TM400ENB is a hardware cryptographic module implemented as a multiple chip embedded module that operates as a line card in Ribbon Communications 's Apollo product line. In the networking parlance it's a transponder with multiplexing and encryption capabilities.

1.2 Security Levels

The module meets the overall requirement of FIPS 140-3 Security Level 3 as detailed below:

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

Table 1: Security Levels

1.3 Additional Information

This security policy is one part of a FIPS 140-3 submission package. The submission package contains:

- Security Policy: This document.
- Algorithm certificates: See section "2.5 Algorithms".
- Functional specification and design documentation: See sections
    - "2.1 Description"
    - "3 Cryptographic Module Interfaces" and
    - The **[TM400ENB-FS]** document.
- User guide: See section "11 Life-Cycle Assurance".
- Finite state machine model: See **[TM400ENB-FSM]** document.
- Configuration item list: See **[TM400ENB-CIL]** document.

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The module is a hardware module that basically acts as a transponder. It exchanges traffic between its client-side ports and line-side ports. Client-side traffic is not encrypted whereas traffic on the line is usually encrypted. One or more client-side traffic streams are multiplexed into a line-side stream. Each client-side stream is independently encrypted.

Module Type: Hardware

Module Embodiment: Multi-Chip Embedded

Cryptographic Boundary:

As a Hardware cryptographic module, the boundary is defined at a physical level. Physically the module comprises a baseboard fitted with a main tamper shield and a small secondary tamper shield serviceable only at Ribbon Communications facilities. This secondary tamper shield guards some PCB signals useful for running board diagnostics & maintenance, but which are also deemed as potentially sensitive. Moreover, the module draws its power from the Apollo backplane and also receives commands/control information & parameters through its backplane Ethernet interface.

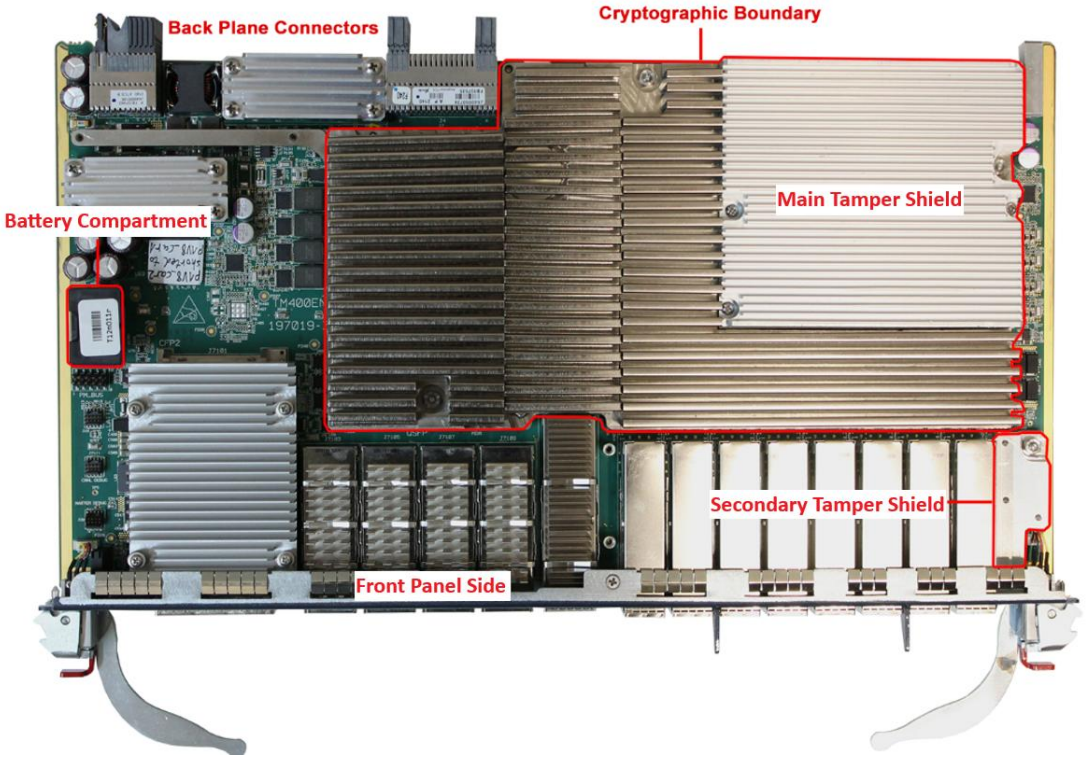


Figure 1: Ribbon Communications TM400ENB Module (Top View)

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

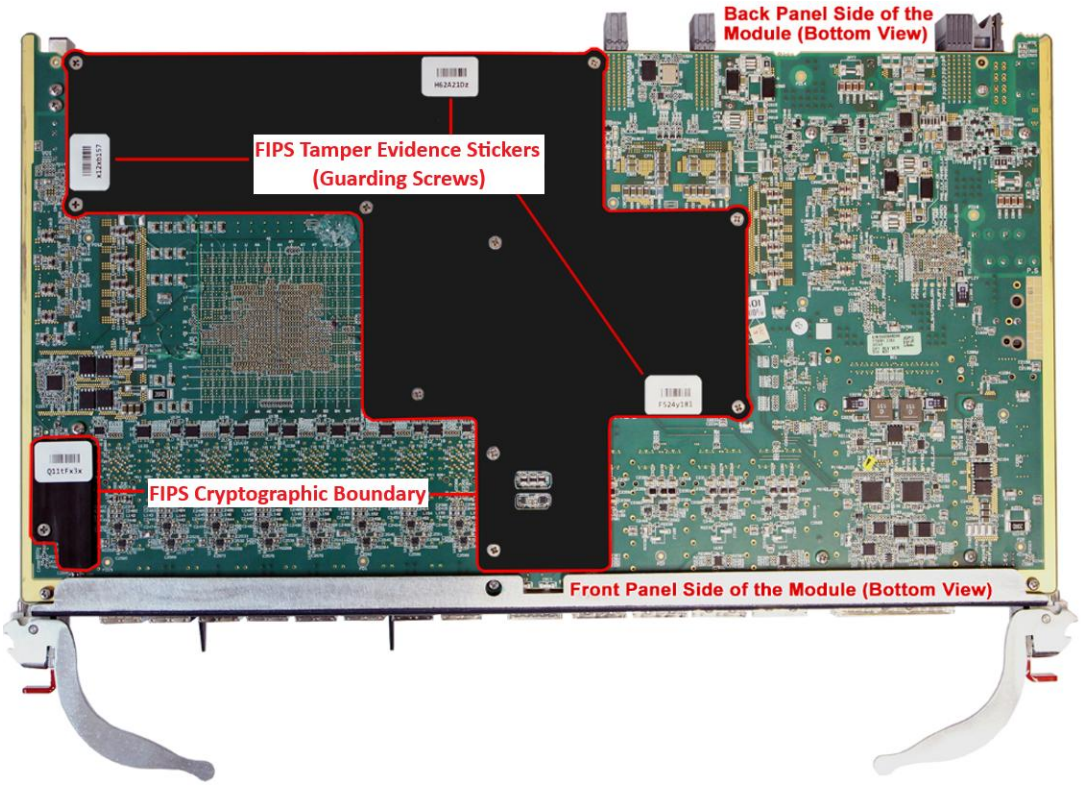


Figure 2: Ribbon Communications TM400ENB Module (Bottom View)

Tested Operational Environment's Physical Perimeter (TOEPP):

The following block diagram provides a system-level overview of the module with encryption application. It covers the control plane as well as the data-plane aspects of the module. The cryptographic boundary is marked as 'TM400ENB' with green outlines:

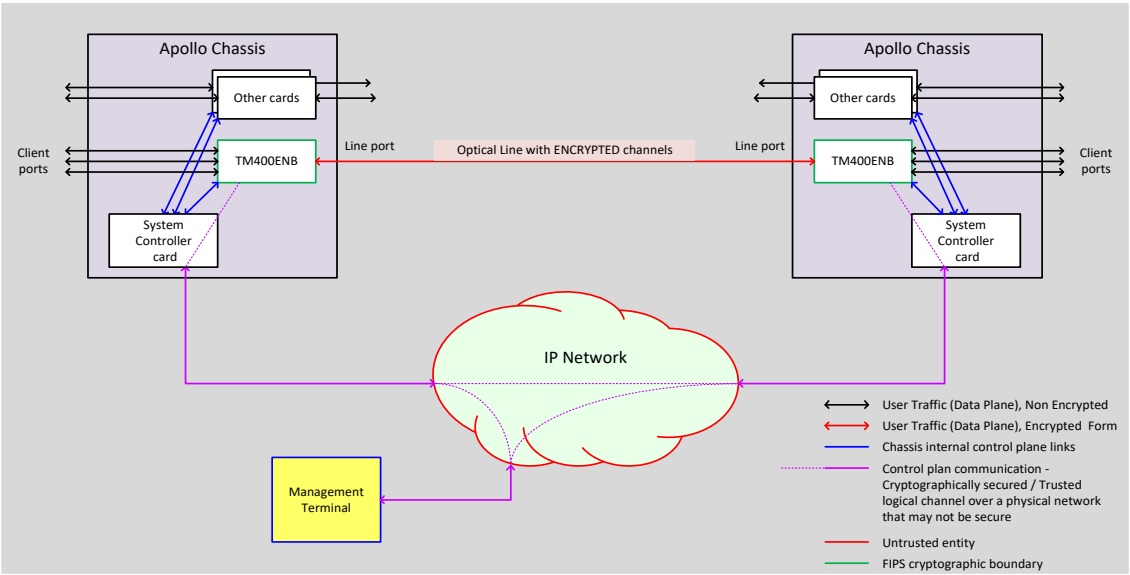


Figure 3: System Level Overview. Block Diagram

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

As shown in the diagram above, the module exchanges traffic in an encrypted form with remote peers reachable through its line-side ports. These remote peers are typically located at great distances and/or reachable across third-party networks, which warrants traffic encryption. Keys for encrypting/decrypting the traffic are established through control plane signalling.

Each line is bidirectional and there are different encryption keys active in each direction at any given time. The module establishes ephemeral encryption keys with the remote peer module through signalling. There is TCP/IP connectivity between peer modules for establishing keys.

The module is composed of the following components:

- **Digi-G5**: It is a framer, multiplexer and client data encryption device whose hardware version is PM6010B1-FEI.
- **SPI boot flash**: It is attached to the Digi-G5 to hold its boot software. Its hardware version is MT25QU128ABA1EW9-0SIT.
- **CFPGA-1**: This is the control FPGA-master. It Mediates control interfaces between various components on the board. Its hardware version is 10CL080YF780I7G and its firmware version is EA01.
- **CFPGA-2**: This is the control FPGA-slave whose hardware version is 10CL016YF484I7G and firmware version is AE01.
- **TOD-RAM**: It is a battery Backed-Up RAM that holds the AES-256 Key-Encryption-Key and a flag for tamper indication with hardware version DS1685E-5+.
- **TCPM-2**: Module controller with version X66233 Rev.A03. It contains a CPU (with hardware version LS1026A) that manages the various configurations and communicates with the system card (RCP) and Ethernet Switch (with hardware version 98DX106-B0-LKJ1C000) that is used to connect with 2 potential RCP cards through the system backplane.
- **IDQ Entropy source**: Quantum theory-based TRNG Entropy source with hardware version IDQ250C2.
- **CPLD**: It is a Pre-boot Programmable logic with hardware version 10M08SAU169C8G and firmware version EA04, that:
    - Controls the module before software is downloaded from the system controller card.
    - Holds CO_pwd on an internal flash memory.
    - Controls a flash memory that holds the module's certificates and encrypted private key.
- **SPI flash**: It is controlled by CPLD. Holds the module’s certificates and encrypted module private key. Its hardware version is GD25LQ32DWIGR.
- **Tamper sensor circuitry**: Upon tamper event (releasing any of the tamper cover screws):
    - Deletes the content of the TOD-RAM automatically.
    - Indicates CPLD tampering, which deletes the CO_pwd.

  If tamper occurs when the module is not powered – it only erases the tamper flag in the TOD-RAM.

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
TM400ENB	D.1	V13.5.1.0.+	LS1026A(ARM64)	TM400ENB is a muxponder module with line side encryption capability. A client signal is encrypted before it's transmitted out of the line port.

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
				Similarly, in the reverse direction the client signal retrieved from OTN frames is decrypted before it's forwarded to the client-side port. The only exception to this is bypass-mode configurable per-client signal. In the bypass mode client signals are directly mapped-to/ de-mapped-from line signal without encryption/ decryption.

Table 2: Tested Module Identification – Hardware

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

N/A for this module.

Tested Module Identification – Hybrid Disjoint Hardware:

N/A for this module.

Tested Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

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

N/A for this module.

2.3 Excluded Components

All components outside the tamper shields are deemed non-critical from a FIPS perspective. These include pluggable optics, back-plane connectors, a serial port, a faceplate, a power-supply, programmable glue logic, LEDs, etc. Malfunctioning of one or more of these components will likely affect the service availability but will not compromise the cryptographic operativity (such as protected CSPs or implemented algorithms) of the module.

The following depiction covers the main board layout including the tamper cover.

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

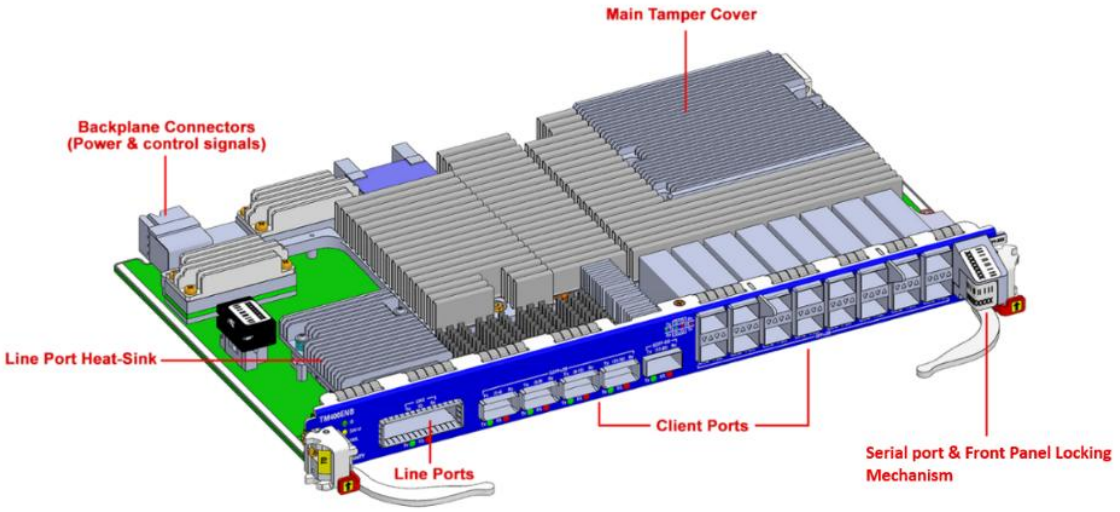


Figure 4: Ribbon Communications TM400ENB Board Assembly

2.4 Modes of Operation

Modes List and Description:

The table below details the Modes of Operation supported by the module.

Mode Name	Description	Type	Status Indicator
Approved Mode	The module only supports approved services	Approved	The module only supports this mode of operation. Therefore, it works in this mode once it is correctly installed and initialized by the CO.

Table 3: Modes List and Description

The module only operates in Approved mode. It does not implement non-approved cryptographic algorithms or a degraded mode of operation.

2.5 Algorithms

Approved Algorithms:

The table below lists all the Approved Algorithms supported by the module.

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A7386	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CTR	A7386	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CTR	C1410	Direction - Encrypt Key Length - 256	SP 800-38A
AES-GCM	A7386	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.2 Key Length - 128, 192, 256	SP 800-38D

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Algorithm	CAVP Cert	Properties	Reference
AES-GMAC	C1410	Direction - Decrypt, Encrypt IV Generation - External Key Length - 256	SP 800-38D
Counter DRBG	A7386	Prediction Resistance - No, Yes Mode - AES-256 Derivation Function Enabled - No, Yes	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-5)	A7386	Curve - P-256, P-384, P-521 Secret Generation Mode - testing candidates	FIPS 186-5
HMAC-SHA2-224	A7386	Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA2-256	A7386	Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA2-384	A7386	Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512	A7386	Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A7386	Domain Parameter Generation Methods - P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KDF SP800-108	A7384	KDF Mode - Counter Supported Lengths - Supported Lengths: 8-4096 Increment 8	SP 800-108 Rev. 1
KDF SSH (CVL)	A7386	Cipher - AES-128, AES-192, AES-256 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
RSA KeyGen (FIPS186-5)	A7386	Key Generation Mode - probableWithProbableAux Modulo - 2048, 3072, 4096, 8192 Primality Tests - 2powSecStr Private Key Format - standard	FIPS 186-5
RSA SigGen (FIPS186-5)	A7386	Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5	FIPS 186-5
RSA SigVer (FIPS186-5)	A7385	Modulo - 2048, 4096 Signature Type - pkcs1v1.5	FIPS 186-5
RSA SigVer (FIPS186-5)	A7386	Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5	FIPS 186-5
SHA2-224	A7386	Message Length - Message Length: 0-51200 Increment 8	FIPS 180-4
SHA2-256	A7385	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4
SHA2-256	A7386	Message Length - Message Length: 0-51200 Increment 8	FIPS 180-4
SHA2-384	A7386	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-512	A7386	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4

Table 4: Approved Algorithms

Vendor-Affirmed Algorithms:

The table below lists all the Vendor-Affirmed Algorithms supported by the module.

Name	Properties	Implementation	Reference
CKG	Key Type:Symmetric and Asymmetric	N/A	According to SP800-133r2 Section 4, example 1

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Table 5: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

The module does not support any Non-Approved, Allowed Algorithms in the Approved Mode of operation.

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

The module does not support any Non-Approved, Allowed Algorithms with No Security Claimed in the Approved Mode of operation.

N/A for this module.

Non-Approved, Not Allowed Algorithms:

The module does not support any Non-Approved Algorithms that are not Allowed in the Approved Mode of operation.

N/A for this module.

2.6 Security Function Implementations

The table below lists the Security Function Implementations supported by the module.

Name	Type	Description	Properties	Algorithms
Traffic Encryption and Decryption	BC-UnAuth	Encryption and decryption of the traffic sent by or received from the line-side port when it is configured		AES-CTR: (C1410) Key Length: 256 bits key Reference: SP 800-38A
Traffic Authentication	MAC	MAC generation and verification of the traffic sent by or, received from the line-side port when it is configured		AES-GMAC: (C1410) Key Length: 256 bits key Reference: SP 800-38D
SSPs encryption	BC-UnAuth	Encryption of the stored CSPs once they are generated or loaded into the module (M_Public and M_Private)		AES-CBC: (A7386) Key Length: 256 bits key Reference: SP 800-38A
SSPs Auth Encryption	BC-Auth	Authenticated encryption of the stored CSPs once they are generated or loaded into the module (M_Public and M_Private)		AES-GCM: (A7386) Key Length: 256 bits key Reference: SP 800-38D
SSH traffic encryption	BC-Auth	Encryption of the SSH traffic when the operators access to		AES-CTR: (A7386) Key Length: 128, 192, 256 bits key Reference: SP 800-

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Name	Type	Description	Properties	Algorithms
		the module via SSH session		38A AES-CBC: (A7386) Key Length: 128, 192, 256 bits ke Reference: SP 800-38A AES-GCM: (A7386) Key Length: 128, 192, 256 bits keys Reference: SP 800-38D HMAC-SHA2-256: (A7386) Reference: FIPS 198-1 HMAC-SHA2-512: (A7386) Reference: FIPS 198-1 SHA2-256: (A7386) Reference: FIPS 180-4 SHA2-512: (A7386) Reference: FIPS 180-4
RSA module's key pair generation	AsymKeyPair-KeyGen CKG	Generation of M_Private and M_Public keys and M_Cert		RSA KeyGen (FIPS186-5): (A7386) Modulus Size: 2048, 3072, 4096 and 8192 bits References: FIPS 186-5; Key Generation mode A.1.6 Counter DRBG: (A7386) Mode: AES-256 Reference: SP 800-90A CKG: ()
KAS-ECC (KBKDF)	KAS-Full	ECDHE key establishment performed automatically by the module prior to sending traffic via the line-port to a peer module. The computed shared secret is utilized as	IG:IG D.F Scenario 2, path (2), split Key confirmation:No Key derivation:KBKDF [SP 800-108] (separately tested) Caveat:Key establishment	KAS-ECC-SSC Sp800-56Ar3: (A7386) Domain Parameter Generation: P-521 Reference: SP 800-56Arev3 ECDSA KeyGen (FIPS186-5): (A7386) Curves: P-521

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Name	Type	Description	Properties	Algorithms
		input of the KBKDF to derive the HEK and HDK keys. Scheme: ephemeralUnified, KAS Role: Initiator, Responder	methodology provides 256 bits of security strength	Reference: FIPS 186-5 KDF SP800-108: (A7384) KDF Mode: Counter Mode MAC Mode: HMAC-SHA2-224, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512 Reference: SP 800-108rev1 HMAC-SHA2-224: (A7386) Reference: FIPS 198-1 HMAC-SHA2-256: (A7386) Reference: FIPS 198-1 HMAC-SHA2-384: (A7386) Reference: FIPS 198-1 HMAC-SHA2-512: (A7386) Reference: FIPS 198-1 SHA2-224: (A7386) Reference: FIPS 180-4 SHA2-256: (A7386) Reference: FIPS 180-4 SHA2-384: (A7386) Reference: FIPS 180-4 SHA2-512: (A7386) Reference: FIPS 180-4
KAS-ECC (SSH)	KAS-Full	ECDHE key establishment performed automatically by the module when a new SSH session is established as a consequence of an operator is accessing to the	IG:IG D.F Scenario 2, path (2), split Key confirmation:No Key derivation:KDF SSH (separately tested) Caveat:Key establishment methodology	KAS-ECC-SSC Sp800-56Ar3: (A7386) Domain Parameter Generation: P-256, P-384, P-521 Reference: SP 800-56Arev3 ECDSA KeyGen (FIPS186-5): (A7386)

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Name	Type	Description	Properties	Algorithms
		module via SSH.Scheme: ephemeralUnified, KAS Role: Initiator, Responder	provides between 128 and 256 bits of security strength	Curves: P-256, P-384, P-521 Reference: FIPS 186-5 KDF SSH: (A7386) Reference: SP 800-135rev1
Peer module authentication	DigSig-SigGen DigSig-SigVer SHA	Authentication between peer modules. It requires to sign and verify a challenge produced internally by each peer involved in the communication	Modulus Size:2048, 3072, 4096, 8192 Hash:SHA2-256, SHA2-384, SHA2-512	RSA SigGen (FIPS186-5): (A7386) Modulus Size: 2048, 3072, 4096 and 8192 bits Signature Type: PKCS 1.5 Hash Algorithm: SHA2-256, SHA2-384, SHA2-512 Reference: FIPS 186-5 RSA SigVer (FIPS186-5): (A7386) Modulus Size: 2048, 3072, 4096 and 8192 bits Signature Type: PKCS v1.5 Hash Algorithm: SHA2-256, SHA2-384, SHA2-512 Reference: FIPS 186-5 SHA2-256: (A7386) Reference: FIPS 180-4 SHA2-384: (A7386) Reference: FIPS 180-4 SHA2-512: (A7386) Reference: FIPS 180-4
Firmware integrity verification	DigSig-SigVer SHA	Verification of the firmware integrity performed by the Boot-Rom during the pre-operational self-tests		RSA SigVer (FIPS186-5): (A7385) Modulus Size: 4096 bits Signature Type: PKCS v1.5 Hash Algorithm: SHA2-256

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Name	Type	Description	Properties	Algorithms
				Reference: FIPS 186-5 SHA2-256: (A7385) Reference: FIPS 180-4
CKG	CKG DRBG ENT-ESV	The module employs DRBG based on AES-CTR to generate the KEK utilized by the module to protect the encrypted SSPs		CKG: () Counter DRBG: (A7386) Mode: AES-256 Reference: SP 800-90A

Table 6: Security Function Implementations

2.7 Algorithm Specific Information

AES-GCM

AES-GCM IV is generated internally and entirely random according to resolution 2 in FIPS 140-3 IG C.H. The module supports internal IV generation using the module's approved DRBG. The IV is at least 96 bits in length per [SP800-38D].

RSA

In case of RSA key pair generation, the module implements 128 Miller Rabin tests that are more than the minimum value of 25 tests required by the IG C.F.

According to IG C.F, the module implements an untested RSA modulus size (8192 bits) for signature generation and verification because no CAVP tests are available for this particular size.

2.8 RBG and Entropy

The module uses an [SP 800-90Arev1] compliant OpenSSL CTR-DRBG module for the generation of random numbers. Seeding of the CTR-DRBG is done repeatedly every 60 minutes by default. This period is configurable by the user via the DRBG shell prompt.

The seed for the CTR-DRBG is obtained from Quantis' IDQ chip QRNG which provides 384 quantum-based entropy bits. Internally to the CTR-DRBG, there are two separate DRBG sources, each of them seeded separately, and their outputs are XORed to provide the final random number output. Quantum random number generator (QRNG) chips exploit the fact that the number of photons emitted by a common light source fluctuates randomly.

While the two internal DRBGs are constantly free-running, whenever the software calls for a random number, their current outputs are XORed in the CTR-RBG OpenSSL module and the final output is provided.

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

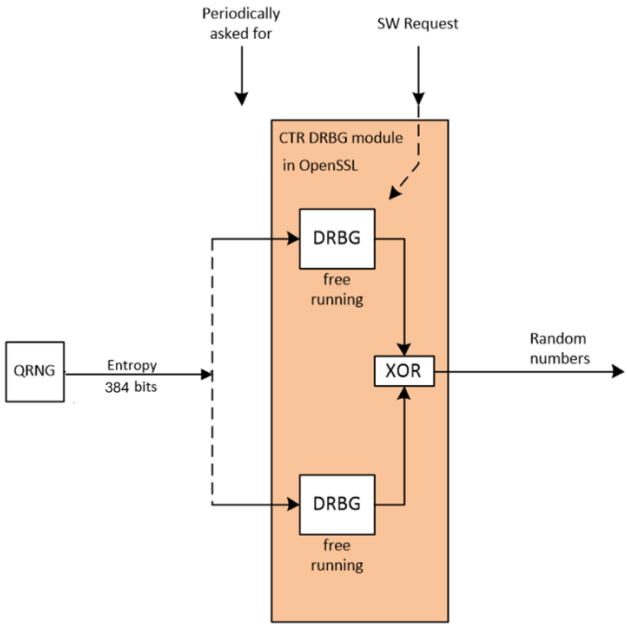


Figure 5: Random Number Generator

Cert Number	Vendor Name
E63	ID Quantique

Table 7: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
IDQ Quantis IID QRNG	Physical	IDQ250C2	2	1.75	N/A

Table 8: Entropy Sources

The module's entropy length is 384 bits. Currently, all requests for random numbers in the module are 384-bit length.

The module utilizes the CTR-DRBG to generate symmetric keys, RSA public/private keys, and necessary parameters to carry out the ECDH key establishment process.

2.9 Key Generation

The module generates Keys and SSPs in accordance with FIPS 140-3 IG D.H. The module performs Cryptographic Key Generation (CKG) as per SP 800-133rev2 (vendor affirmed). The resulting symmetric keys and the seeds for RSA public/private keys and ECC key pair generation (according to Section 4, 5.1, 5.2, 6.1, 6.2.1 and 6.2.2 of [SP 800-133 rev2]) are the output of the result of calculating the XOR of two separate and independent DRBG sources as detailed in section "2.8 RBG and Entropy".

The module also implements the following key derivation functions:

- KBKDF Key Derivation according to [SP 800-108] to derive symmetric keys.
- KDF SSH according to [SP 800-135rev1] to derive symmetric keys.

Besides, the module does not output any intermediate key generation value.

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

2.10 Key Establishment

The module implements the following SSP establishment related services in the Approved mode:

- ECDHE for the line-port key establishment

The module implements a key establishment process according to FIPS 140-3 IG D.F Scenario 2 path (2) to establish symmetric keys with 256 bits in length that will be used to encrypt/decrypt the sent/received traffic to/from peers.

- ECDHE for the establishment of SSH session

The module implements a key establishment process according to FIPS 140-3 IG D.F Scenario 2 path (2) to establish symmetric keys with 128, 192 or 256 bits in length that will be used to encrypt/decrypt the sent/received traffic via the SSHv2 channel established via the serial port when the CO and Human operator are authenticated.

2.11 Industry Protocols

SSHv2 Protocol

The module implements the SSHv2 protocol. The SSH KDF Component CVL algorithm is only utilized in the context of the SSHv2 protocol. This is enforced internally by the module, and therefore it is not utilized for other purposes as required by FIPS 140-3 IG 2.4.B. No parts of the SSH protocols, other than the KDF, have been tested by the CAVP or CMVP.

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

The following picture shows the ports and interfaces available on the TM400ENB board:

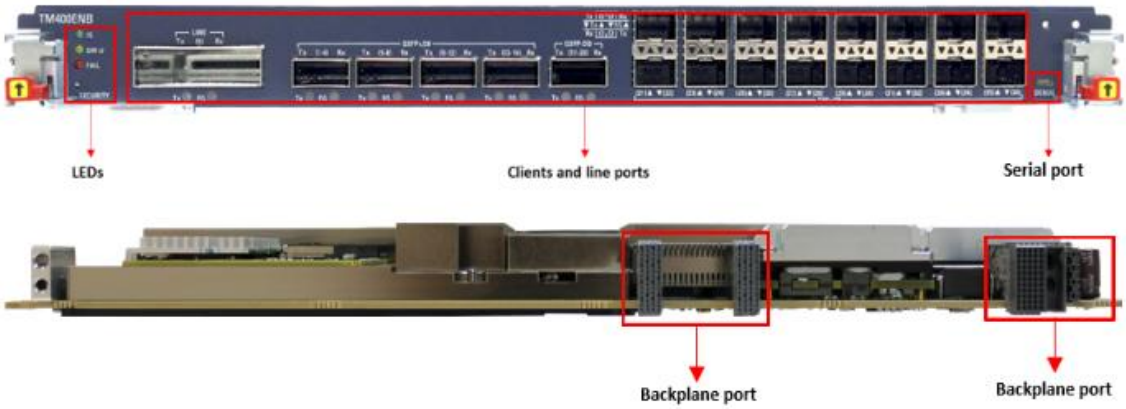


Figure 6: Ports and interfaces on TM400ENB in front and back sides

The module has three different ports that can be accessed from the front panel of the TM400ENB board and an additional one that is an internal port between the module and the System card:

- **Data Ports**

  The module has two types of data ports: client-ports and a line-port. There is a provision for 36 client ports and 1 line port.

  The 36 client ports are comprised of various types of physical interfaces and data signals and rates. The encryption engine for all streams is the same. It's not mandatory to populate all the client ports. On the contrary, the pluggable optics allow customers to only populate a subset of available ports. Additionally, this scheme allows a mix and match of different types of signals (OTN/Ethernet/Fiber-Channel) in a given deployment.

- **Serial Port**

  The serial port is required for the initial CO_pwd configuration when a module is received from the factory. Beyond this initial step, the serial port can be kept sealed as a security measure. That way any unauthorized access to the serial port can be monitored. However, covering the serial port is not mandatory for FIPS compliance considering that it serves as an output status in conjunction with the front panel LEDs.

  Each time a module is powered up, a firmware menu is presented through the serial port. The CO can interrupt the boot process, provide the CO_pwd, and run privileged commands to perform initial key loading and management of SSPs. After the boot phase, a regular login prompt can be seen through the serial port. Regular (non-CO) operators can perform login authentication using their password.

  In other words, beyond the initial CO_pwd configuration, authentication (by the CO or by operators) is always required in order to perform CO related tasks or other tasks. The CO and users have different roles and different access privileges to the module. In short, the CO is responsible for the physical security of the module and managing its persistent CSPs; while users are responsible for service configuration, monitoring, and log collection. Users do not have the access rights to modify the CSPs.

- **Management Ethernet**

  Ribbon Communications TM400ENB Encryption Module is a line card in Apollo chassis that is configured & monitored through the System card (sometimes called the RCP: Route Control Processor in Ribbon Communications literature) in the chassis. This system card sends various image files, boot parameters,

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

command and configuration parameters to each Ribbon Communications TM400ENB Encryption Module in its chassis.

There is an intra-chassis Ethernet link running between the System card and any line card module. This Ethernet link is not accessible to end users; it is part of the backplane signals of the Apollo chassis.

SSH Interface can be used to load the initial CSPs (instead of the serial port). Under normal operating conditions, SSH is not required since there is a control messaging channel running between the embedded applications running on the system card and Ribbon Communications TM400ENB Encryption Module for service provisioning and monitoring.

- **Front Panel LEDs**

  There are six different kinds of LEDs that are used as status output interfaces for different purposes as detailed in the table below.

The following table specifies the association between the module's physical ports and the logical interfaces defined by the FIPS 140-3 standard:

Physical Port	Logical Interface(s)	Data That Passes
Client Port 1-36. See the table below to consult the specific connectors	Data Input Data Output	These ports are located on the front panel. Users may provision all or only a subset of client ports at a given time. Each provisioned client port runs data traffic to a customer's premises without encryption. Traffic from a client port is cross-connected to the line port of the module
Line Port (0). Connector (J7101)	Data Input Data Output	This port is located on the front panel. The port exchanges OTN data traffic with a remote-peer. This traffic is encrypted (except for the bypass mode) using AES-CTR in conjuction with AES-GMAC
Serial. Connector (J10)	Control Input	Used to configure the CO_pwd, CSPs, and certificates
Backplane port - Ethernet /Logical Control Channel. Connector (J4)	Control Input	This is a TCP/IP-based logical control messaging channel that uses the management Ethernet physical link between the system card and the module. It is used by the software application to control de module. There can be up to 2 System cards in a chassis (active & standby). Only one is active at a given time. There is a point-to-point Ethernet link between each system card and a given module. In other words, the module has 2 management Ethernet ports (one to each System card), only one of which can be active at any given time
Backplane port - Control Signals. Connector (J4)	Control Input Status Output	The system card can perform certain control operations on the module by exercising control signals such as reset and shutdown. In addition, there are few lines to connect to the adjacent TM400ENB module for 1:1 module protection signalling through which each module sends its failure status to the other module
Serial. Connector (J10)	Status Output	The serial port is utilized by the module for several purposes: - Indicate the state of the module every time it reaches a new state with the following format: "STATE: State_name"; - Provide the operator with additional information such as causes of error or indications
IS LED. Connector (DS33(G))	Status Output	This is a green-coloured LED on the front panel utilized by the module to indicate the kind of error according to the table of Error States. Moreover, this LED also blinks depending on the module's internal operativity
SW-U LED. Connector (DS33(Y))	Status Output	This is a yellow-coloured LED on the front panel utilized by the module to indicate the kind of error according to the table of Error States. Moreover, this LED also blinks depending on the module's internal operativity

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Physical Port	Logical Interface(s)	Data That Passes
FAIL LED. Connector (DS33(R))	Status Output	This is a multi-coloured LED on the front panel utilized by the module to indicate kind of error according to the table of Error States. Moreover, this LED also blinks depending on the module's internal operativity
Security LED. Connector (CR6)	Status Output	This is a multi-coloured LED on the front panel utilized by the module to indicate kind of error according to the table of Error States. Moreover, this LED also blinks depending on the module's internal operativity
Tx (One LED per port). See the table below to consult the specific connectors	Status Output	This is a software-controlled green-coloured LED. It is off until the associated port is configured and enabled.
F/L (One LED per port). See the table below to consult the specific connectors	Status Output	This is a red-coloured LED. It's off during normal operation. When on, it indicates associated port failure conditions (voltage/temperature out-of-range, Loss-Of-Signal).
Backplane port - Power input. Connector (J4))	Power	Power supply voltage 48V DC

Table 9: Ports and Interfaces

The following table specifies the Client & Line ports assignment:

Port number	Port Connector Number	Port Tx LED	Port Fail LED
0	J7101	CR23	CR22
1-4	J7103	CR21	CR20
5-8	J7105	CR19	CR18
9-12	J7107	CR17	CR16
13-16	J7109	CR15	CR14
17-20	J7102	CR13	CR12
21	J7111-T	DS17	DS2
22	J7111-B	DS1	DS18
23	J7112-T	DS19	DS4
24	J7112-B	DS3	DS20
25	J7113-T	DS21	DS6
26	J7113-B	DS5	DS22
27	J7114-T	DS23	DS8
28	J7114-B	DS7	DS24
29	J7115-T	DS25	DS10
30	J7115-B	DS9	DS26
31	J7116-T	DS27	DS12
32	J7116-B	DS11	DS28
33	J7117-T	DS29	DS14
34	J7117-B	DS13	DS30
35	J7118-T	DS31	DS16
36	J7118-B	DS15	DS32

Table 10: Client & Line ports assignment

Although the module is able to communicate with other modules, it does not implement a control output interface since such communication does not encompass controlling commands or signals to control other modules. Moreover, as detailed in the “4 Roles, Services, and Authentication” section, the module does not support a maintenance role, therefore a maintenance interface is not required.

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Moreover, while the module is performing self-test, key zeroization, key generation, or is in an error state, all data output interfaces are inhibited.

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

4 Roles, Services, and Authentication

4.1 Authentication Methods

The following table defines the authentication methods implemented in the module:

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
CO Authentication	Identity-based authentication for the CO role.	The CO_pwd must be [8,20] characters in length, with at least 1 upper case, 1 lower case, and 1 number. With 102 possible values per character, it provides adequately low odds of a random match as per the FIPS specification.	The crypto officer is authenticated by the module using a password of [8, 20] characters in length allowing to choose between 102 possible values for each character (26 upper-case, 26 lower-case, 10 numbers and 40 additional characters provided by 20 keys on the ASCII keyboard (with or without SHIFT) leads to 26+26+40+10 = 102) of the password, hence, the minimum and the maximum possibility that a random attempt succeeds or a false acceptance occurs is P_max=1/(102)^8 and P_min=1/(102)^20. This authentication method complies with the stated in the [SP 800-63B] document for memorized secret authentication.	Moreover, for the CO, after the first authentication failure, the module will take 3 seconds after allowing the CO to perform a new authentication attempt. After the second authentication failure, the module will take 6 seconds after allowing the CO to perform the third authentication attempt. Finally, after the third authentication failure, the module will take 9 seconds to close the CO-Shell and open a new one. Taking into account that this process takes a total amount of 18 seconds (without considering the tipping time), the maximum number of authentication attempts within a minute is 9, therefore, the possibility that a random attempt succeeds or a false acceptance occurs P_max=9/(102)^8 and P_min=9/(102)^20.
System-Card Authentication	System-Card Authentication	As the system card monitors the module's status and provisioned services, performs self-tests and firmware integrity tests, not executing any approved cryptographic algorithm nor managing any CSPs/SSPs - there is	N/A	N/A

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
		no need for authentication as per FIPS 140-3 IG 4.1.A Resolution section bullet d) and e).		
Human Operator authentication	Identity-based authentication for the User role.	The user password must be at least 8 characters in length, with at least 1 upper case, 1 lower case, and 1 number. With 102 possible values per character, it provides adequately low odds of a random match as per the FIPS specification.	This user is authenticated by the module using a password with at least 8 characters in length allowing to choose between 102 possible values for each character (26 upper-case, 26 lower-case, 10 numbers and 40 additional characters provided by 20 keys on the ASCII keyboard (with or without SHIFT) leads to 26+26+40+10 = 102) of the password, hence, the possibility that a random attempt succeeds or a false acceptance occurs is P_max=1/(102)^8. This authentication method complies with the stated in the [SP 800-63B] document for memorized secret authentication.	After configuring the lockout policy as indicated in section 11. The configuration for the authentication failures within a minute is the same as for the CO, therefore, during a minute, the maximum number of authentication attempts is 9, therefore, the possibility that a random attempt succeeds of false acceptance occurs in one minute period is P_max=9/102^8

Table 11: Authentication Methods

The module complies with identity-based authentication requirements for FIPS Security level 3 certification supporting CO and user roles. While multiple users can log on to the module via multiple SSH links in order to get some status information, only a single user (of any role) at any given time can be logged on to the serial port. Once a user successfully logs on to the serial port, the previous user is automatically logged off. Moreover, the module does not provide a maintenance role and enforces authentication when changing roles.

4.2 Roles

The following table define the different roles implemented in the module:

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Identity	CO	CO Authentication
System-Card	Identity	System-Card (User Role)	System-Card Authentication
User	Identity	Human Operator	Human Operator authentication

Table 12: Roles

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

More details about the roles can be found bellow:

1. **CO (Cryptographic Officer role):** CO Is the only person authorized to load CSPs (Initial key loading and SSPs management) into the module.
    a. In order to load/modify these CSPs, the CO must provide a valid CO_pwd on a dedicated CO-Shell in order to be authenticated.
    b. The CO_pwd is originally assigned during module installation. Later on, the CO_pwd can be modified provided the CO can provide the current password.
    c. CO can load the module key pair (M_public and M_private} and X.509 certificates (M_cert and CA_cert) into the module via CO Shell using SSH or via the Serial port.
    d. CO can configure or change the CO_pwd only via direct connection through the Serial port.
    e. Only a single CO shell can be active at any given time (i.e. no concurrent CO operation). This simplifies the implementation and security handling. If a new CO shell is launched and CO credentials are entered through it, the previous active CO shell session is terminated.
2. **System-card (User role):** The system card (RCP) is a software component responsible for monitoring module health, FIPS status, service status, and provisioning services.
    a. It uses a proprietary messaging format to exchange information with the module.
    b. These accesses are made over the trusted intra-chassis Ethernet control-channel.
    c. System-card software cannot modify/substitute/disclose CSPs on the module.
    d. Only one system card/application instance can manage a Ribbon Communications TM400ENB Encryption Module at any given time. Concurrent access is not required and is not supported.
3. **Human operator (User role):** Human operators can log in to the module either over an SSH (Secure Shell) connection or through the console port (i.e. the serial port). They must authenticate by entering a valid user login and password.
    a. Human operator access is supported to collect debug information under abnormal conditions. Multiple human operators can concurrently log into the card and monitor the module state/collect debug data.

Each initialized FIPS module owns a public and private key pair (M_private and M_public). Only the CO can modify it. The public key from this key pair can be read later by CO or Users. However, the private key is never revealed to anybody through any interface. Similarly, the traffic-encryption keys for traffic encryption/decryption of each client port are never revealed to the CO or any other user.

None of the authentication modes described above are persistent across module reboot/reset or power-cycle operations. It must be performed again after any such operation as the results from the previous authentication are erased after reboot/reset or power-cycle.

Feedback of authentication data is not displayed during the authentication process, moreover, authentication information such as operator login is not accessible unless the operator can perform a successful login. The module never reveals the CO_pwd or private-key to any users, including the CO. CO can only gain access to a module if the entered password matches with the previously configured value.

4.3 Approved Services

The table below lists all Approved Services supported by the module. The abbreviations of the access rights to keys and SSPs have the following interpretation:

G = Generate: The module generates or derives the SSP.

R = Read: The SSP is read from the module (e.g., the SSP is output).

W = Write: The SSP is updated, imported, or written to the module.

E = Execute: The module uses the SSP in performing a cryptographic operation.

Z = Zeroize: The module zeroizes the SSP.

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Create new user	This service requires several steps: 1. It is necessary to create the user in the controller card. 2. The user shall log in to the controller card and establish a new password according to the authentication rules of the module. 3. Reset the module (This will make sure that once the app is running, it copies the shadow file from the controller card to the module). After that, the user can log in to the module either using SSH or a serial connection.	Successful completion and possibility of user authentication	Username, password, and user class in the RCP and restart to copy the shadow file into the module	There is no output. The new user can log in and run his/her associated services	None	User - User_pwd: W
Show status	Show the current status of the module according to FSM. It is automatically executed by the module depending on its current state according to the FSM.	Serial port and log file indicating the current status of the module	N/A	The module shows automatically without the user intervention on the current module status via the serial port and log file	None	User
Show version	Show module hardware and firmware	The module outputs the following information through	Command to show the	Shows the module name and	None	User

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	version. The module version can be obtained from the module as detailed below: 1. Connecting to the module via SSH and using the "ver" command to obtain the module name and software version. 2. Using the "run show chassis inventory slot-<slot_number>" where <slot_number> indicates the slot chassis.	the shell for each case (additional information that is not included here is given): "1. Application Version: V13.5.1.0.+; Inventory info for slot-<slot_number>: | Type: TM400ENB (34267) | Hardware Revision: D.1"	module version	software and hardware versions among additional informati on		
Perform Self-Test	Execute pre-operational self-tests. Automatically performed by SW during power-up. The System-Card may initiate Reset using the "run request chassis power reset" command.	Response in shell detailing the following: "Running FIPS POST (power-on self-tests) ... Successfully passed all FIPS self-tests"	Command to cause the reset of the module	If the module executes the self-tests with success, it returns a message via the serial port, otherwise , the module indicates the error state and additional informati on related to via the serial port and log file	None	System-Card
Configure period for	Configuration of the period in days to execute	This function returns a message (as shown in the example below)	Command indicating : - The	Confirmat ion message	None	User

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Periodic Self-Test	the periodic self-tests. The specific command is "set chassis slot <slot_number> tm400enb-m self-test-options self-test-years X self-test-time YY:YY", where <slot_number> indicates the slot to be configured, "X" indicates the years (between 1 and 5) and the "YY:YY" indicates the hour.	via the serial port that indicates the remaining seconds for the following periodic self-test execution ("self_test_remaining_seconds") among other data	period in days (between 1-5 years) - The time to execute it using two digits for hours and two digits for minutes	via serial port. Moreover, once the period ends, the software initiates a module power cycle, which ends up in a pre-operational self-test		
AES key establishment	Negotiation of the symmetric key with remote peer module, resultant from an ECDH key establishment. Upon the configuration of an end-to-end un-encrypted link by the Human Operator, the module performs this as part of link establishment. For this purpose, the following command shall be used: "set chassis slot <slot_number> tm400enb-m port	When the peer is authenticated, the AES Key is established, and, the module starts sending and receiving encrypted traffic via the configured port, the TX LED associated with this port is on (with green color)	The establishment of HEK and HDK requires to exchange the required information to authenticate the peer module based on RSA signature authentication and to perform the key agreement based on ECDH	The establishment of HEK and HDK requires to exchange the required information to authenticate the peer module based on RSA signature authentication and to perform the key agreement based on ECDH	KAS-ECC (KBKDF) CKG	User - ECDH_Priv_K: G,E - ECDH_Pub_K: G,E - KBKDF_MK: G,E - KH_Key: G,E - DRBG Seed: G,E - DRBG Internal Value: G,E - DRBG Key: G,E - HEK: G,W - HDK: G,W

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	<port_number> oduc 1 odu odu2-TPN1 encryption enabled"					
SSH key establisment	Negotiation of the symmetric key to establish an SSH session when an operator is accessing to the module via SSH	The operator is logged with success to the module via SSH	It requires operator to be logged using the serial port and SSH protocol	Successful access to the module	KAS-ECC (SSH) CKG	User - ECDH_Priv_K: G,E - ECDH_Pub_K: G,E - DRBG Seed: G,E - DRBG Internal Value: G,E - DRBG Key: G,E - SSH_KDF_K: G,E - SSH_K: G
Datapath Encryption	Encryption of incoming data on client ports. Upon the configuration of an end-to-end un-encrypted link, the module encrypts user data with the HEK AES key. For this purpose, the following command shall be sent: "set chassis slot <slot_number> tm400enb-m port <port_number> oduc 1 odu odu2-TPN1 encryption enabled".	When the peer is authenticated, the AES Key is established, and, the module starts sending and receiving encrypted traffic via the configured port, the TX LED associated with this port is on (with green color)	Client-side payloads received from the client ports	Client-side payloads are encrypted using AES-CTR and AES-GMAC algorithm and sent to the peer via the line ports	Traffic Encryption and Decryption Traffic Authentication	User - HEK: R,E

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Datapath Decryption	Decryption of outgoing data on client ports. Upon the configuration of an end-to-end un-encrypted link, the module decrypts user data with the HDK AES key. For this purpose, the following command shall be sent: "set chassis slot <slot_number> tm400enb-m port <port_number> oduc 1 odu odu2-TPN1 encryption enabled".	When the peer is authenticated, the AES Key is established, and, the module starts sending and receiving encrypted traffic via the configured port, the TX LED associated with this port is on (with green color)	Line port traffic encrypted with AES-CTR and AES-GMAC	Decrypted line port traffic is output via the required client port	Traffic Encryption and Decryption Traffic Authentication	User - HDK: R,E
CO Password Configuration	Configuration of CO_pwd for authentication into the module. There are two possible methods of using the serial port: - During initial configuration, the module detects that CO user does not exist in the module and offers the possibility of creating one by pressing "P" when it is required by the module. - When the CO	In both situations the module outputs the following message via the serial port: "Password configured. Please remember your password."	The CO_pwd to be configured or modified	Confirmation via CO-Shell	None	Crypto Officer - CO_pwd: W

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	user already exists, the module offers the possibility of changing the current CO_pwd every time it is powered-on. This can be done by pressing "P" when it is required by the module. Note: Both cases require to be connected to the module via serial port.					
Zeroization service	Zeroization of the SSPs stored within the module. This is done by using CO-Shell command via serial port. The specific command is "zeroize". Note: In addition, the module offers automatic zeroization when the HEK and HDK keys are rotated and in case of tamper detection as detailed in the "9.3 SSP Zeroization Methods" section.	During zeroization process, the security LEDs on the front panel blink in Red with the pattern 1 sec on/1 sec off and the following response via CO-Shell: "Please wait !!!Zeroize command in process DeleteCaCert Successful. Delete RSA Key pair Successful. Format Flash Successful. Zeroize LED Set. passwd, shadow files removed. Line and Client port Laser off successfully. Zeroization command Successful." After completion of the zeroization process, the Security LED blink in Orange with the pattern 2.5 sec on/2.5 sec off.	Command to execute the zeroization	While performing the zeroizaton, the security LED blinks in Red with the 1 sec on/1 sec off pattern and the message specified in indicator column. After completing the zeroization, the security LED blinks in Orange with the 2.5 sec on/2.5	None	Crypto Officer - M_Private: Z - M_Public: Z - M_cert: Z - CA_cert: Z - KEK: Z - User_pwd: Z

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
				sec off pattern		
Selective Bypass	Enable/disable bypass on specific client ports upon the configuration of an end-to-end un-encrypted link by the Human Operator. For this purpose, the Human Operator sends the following command via the serial port: "set chassis slot <slot_number> tm400enb-m port <port_number> oduc 1 odu odu2-TPN1 encryption disabled".	An indication for this service is recorded in the log file detailing "<ChannelId port_id> Enable PassthruModencryption". Moreover, the module will start sending traffic to the peer via the conjured link	Client-side payloads received from the client ports	Client-side payloads are sent without encryption via the line ports to the peer	None	User
Firmware integrity check	Perform SW & FW integrity and authenticity tests based on RSA signature verification based on 4096 modulus withs SHA-256 message digest. Automatically performed by the Boot-ROM during power-up. System-Card may initiate Reset using the "run request chassis power reset" command or resetting the	Considering that the firmware integrity check is successfully performed if the module executes the pre-operational self-tests, the output provided by the module via serial port is the same as for the "Perform self-test" service: "Running FIPS POST (power-on self-tests) ... Successfully passed all FIPS self-tests"	Same as performing the self-test service	If the module executes the self-tests with success, it returns a message via the serial port, otherwise, the module enters in error state. Moreover, the current error state and additional	Firmware integrity verification	System-Card - Boot_Public: R,E

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	module, by which self-test is performed automatically.			informati on related to it are output via the serial port and log file		
Generate KEK	Generate Key Encryption Key and store it in memory-backed-up RAM. It is automatically executed by the module after performing "Generate RSA keys" or "SSP external upload" services to encrypt the generated/load ed key pair.	Successful completion and the fact that the module does not go either to "General error state" in RSA PCT fails or "SSPs Entry or Generation" state if an error occurs during the generation or loading of the RSA key pair	M_privat e, Mpublic, and M_Cert in the case they are loaded into the module instead of being generated	Same as Generate RSA Keys or SSP external upload services	CKG	Crypto Officer - DRBG Seed: G,E - DRBG Internal Value: G,E - DRBG Key: G,E - KEK: G,W
Generate RSA keys	Generate RSA module key pair via the CO-Shell using the "GenerateKeyP air" command to generate the key pair.	Response in the CO-Shell showing the following message: "Keys generated successfully"	N/A	Response via the CO-shell	RSA module's key pair generatio n CKG	Crypto Officer - DRBG Seed: G,E - DRBG Internal Value: G,E - DRBG Key: G,E - M_Privat e: G,W - M_Public : G,W
SSP external upload	Upload SSPs via the CO-Shell on the Serial port console via an SSH channel using the "LoadCaCertific ate" command to load the	Response in the CO-Shell for each specific command: CA Certificate loaded successfully Public Certificate loaded successfully Private Key successfully loaded	CA_Cert, M_privat e, M_Public, and M_Cert are loaded	Response via the CO-shell	None	Crypto Officer - CA_cert: W - M_cert: W - M_Privat

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	CA_Cert, the "LoadPublicCertificate" command to load the M_Cert, and "LoadPrivateKey" command to load the M_private key.		into the module			e: W - M_Public: W
Peer authentication	Peer authentication based on generating a challenge by performing digital signature generation and digital signature verification. It is an automated process that occurs in every key exchange as part of link establishment. For this purpose, the Human operator sends the following command: "set chassis slot <slot_number> tm400enb-m port <port_number> oduc 1 odu odu2-TPN1 encryption enabled".	When the peer is authenticated, the AES Key is established, and, the module starts sending and receiving encrypted traffic via the configured port, the TX LED associated with this port is on (with green color)	Peer M_Cert is received to perform the authentication	M_Cert is sent to the peer	Peer module authentication	User - M_Private: R,E - CA_cert: R,E
SSH session encryption	Encryption of the SSH traffic when an operator is accessing to the module via SSH after performing the	The CO or Human Operator is logged with success to the module via SSH	It requires the CO or human user to be logged using the serial port and SSH protocol	Successful access to the module	SSH traffic encryption	User - SSH_K: R,E

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	key establishment					
Symmetric Encryption/Decryption	This service is used to encrypt/decrypt the M_private key using KEK. By default, AES-CBC is used by default although AES-GCM could also be utilized. It occurs as part of the loading/generation of the M_private key. Once it is loaded using the "LoadPrivateKey" command or generated using the "GenerateKeyPair" command the module encrypts it using the KEK.	Same as Generate RSA Keys and SSPs External Upload services because when the keys are either generated or uploaded, they are automatically encrypted and the output of both services means that the keys are stored in an encrypted form in the module	The M_private key to be encrypted	Same as Generate RSA Keys or SSP external upload services	SSPs encryption SSPs Auth Encryption	Crypto Officer - M_Private: R,E - KEK: R,E

Table 13: Approved Services

4.4 Non-Approved Services

The module does not support any Non-Approved Services.

N/A for this module.

4.5 External Software/Firmware Loaded

The module does not load external software or firmware..

4.6 Bypass Actions and Status

As detailed in the Approved Services Table, the module supports bypass service to disable the encryption of the client interfaces on the line port. It can be initiated by the Human operator. An indication for this operation is recorded in the log file detailing “<ChannelId port_id> Enable PassthruMode” where port_id indicates the port that is going to be working in bypass mode.

Bypass can be provided by Human operator (user) via the management software (EMS or Muse), that interacts with the system card (RCP), which in turn sends a command to the module to disable encryption/decryption. The operator

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

asks the module to disable the encryption/decryption on a certain channel. The module will then ask the operator for approval of this operation before it sends the appropriate command to the system card.

Since the module supports bypass capability, the required self-test to check the correct operativity of the bypass is detailed in section “10 Self-Tests”.

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

5 Software/Firmware Security

5.1 Integrity Techniques

The Boot-ROM software is responsible for checking the module's software/firmware integrity based on the RSA signature verification cryptographic algorithm based on 4096 bits modulus with SHA-256 message digest during the pre-operational self-tests as detailed in section "10.1 Pre-operational Self-test".

The key used to perform the software/firmware verification is the Boot_Public that resides on the CPU ROM. The private key (Ribbon's Private key) associated with Boot_Public key resides outside the module.

Moreover, the module does not support software/firmware loading service, therefore, a conditional software/firmware loading test is not required.

5.2 Initiate on Demand

The module allows the operator (user role) to execute the software/firmware integrity check on demand by rebooting the module using the **"run request chassis power reset"** command. In case of failure, the module enters in error state.

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Non-Modifiable

The module runs Ribbon Communications customized version of the embedded Linux operating system (branded as MOS: Magnum OS, version 9.6MZ06; Linux kernel version 4.19.68-0). MOS doesn't support the ability to add/delete/modify applications dynamically (i.e. in production environments). Ribbon Communications releases and controls the operational firmware image.

The module (i.e. Boot-ROM v5.0.36+ application) fetches the MOS image file from the System card, verifies its digital signature, and then executes it. The module software cannot be modified by any operator, and it does not support firmware/software loading, therefore, it is considered as 'non-modifiable operational environment'.

The System card uses a proprietary messaging mechanism to interact with user space application processes running on the module. This mechanism facilitates the configuration and monitoring of encryption services on the module but doesn't alter the MOS itself.

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

7 Physical Security

Ribbon Communications TM400ENB Encryption Module functions as a line card in Ribbon Communications Apollo chassis. It falls under the category of "multi-chip embedded cryptographic modules" for SL3. In that context, it provides physical tamper protection and environmental failure protection (EFP).

7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
Strong tamper cover	Every month	The CO must perform a visual inspection of the metallic cover to ensure it has not been manipulated or damaged.
Tamper seals	Every month	The CO must perform a visual inspection of the tamper seals to ensure it has not been manipulated, damaged, or replaced (Verifying they are correctly encoded).
Tamper detection and zeroization circuitry	Every month	The CO must check that the module is working under normal conditions. This will require the CO to authenticate into the module (ensuring the module has not been tampered with and that the battery has not lost power).

Table 14: Mechanisms and Actions Required

1. The module provides evidence of tampering through multiple means:
    a. The primary tamper-evidence mechanism is through 7 tamper evident seals factory-applied across critical surfaces of the module. The tamper evident seal shall be installed for the module to operate in approved mode of operation.
    b. There is a strong tamper cover that is mated (and sealed using the above seals and other means) with the board. This cover prevents visual, electrical, or mechanical access to sensitive components on board.
    c. The module has embedded electronic tamper detection and response circuitry.
        i. If there is a tamper event (called main tamper) while the module is powered up, this circuitry activates instantaneous tamper response as follows:
            1. Normal operation of the h/w and firmware is immediately halted.
            2. The KEK and CO_pwd stored on board are permanently zeroized.
            3. An additional, persistent hardware marker is set which prevents initialization or re-installation of the module.

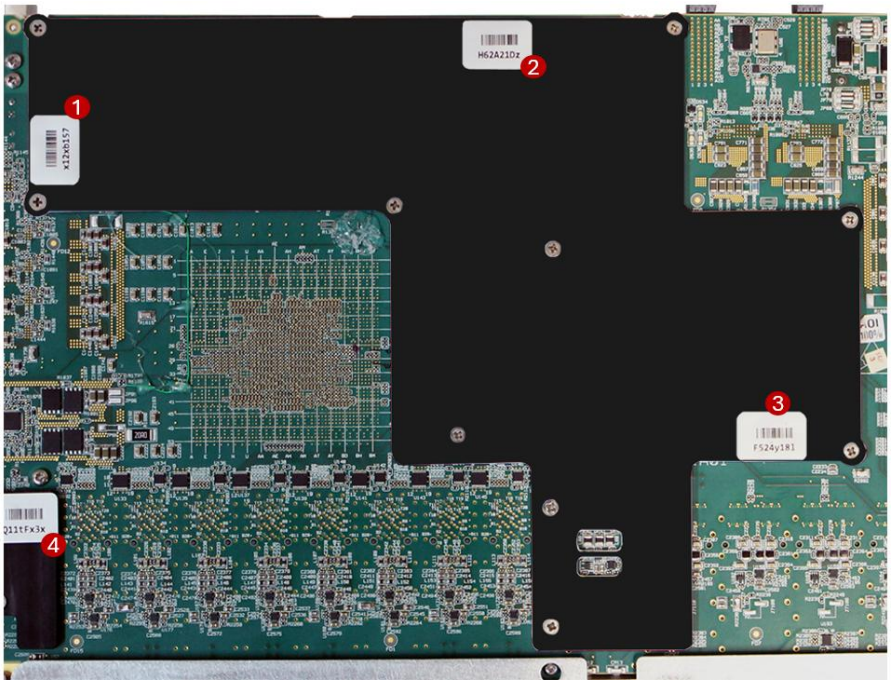
        The module under these conditions must be returned to the factory. Power-cycling the module doesn't restore it to working conditions.
        ii. If there is an attempted tampering (called secondary tamper) while the module is powered down, there is battery-backed electronic circuitry to remember this event using a flag in the memory. If the module is powered up subsequently, it fails to boot without CO's authentication and consent.
        iii. Note that this flag indication can also be set if the on-board battery has lost its power while the module was not powered. In such case, it is required that the CO shall replace the battery and then give his consent to boot.
2. The module also has a locking and sealing mechanism that prevents removal from its slot after installation. This is achieved as follows:
    a. After seating the module in its chassis, a mechanical cover is screwed over the front panel.
    b. Then a tamper-detection seal is applied across the cover. This prevents unauthorized removal of the module from its slot without visual tamper detection.

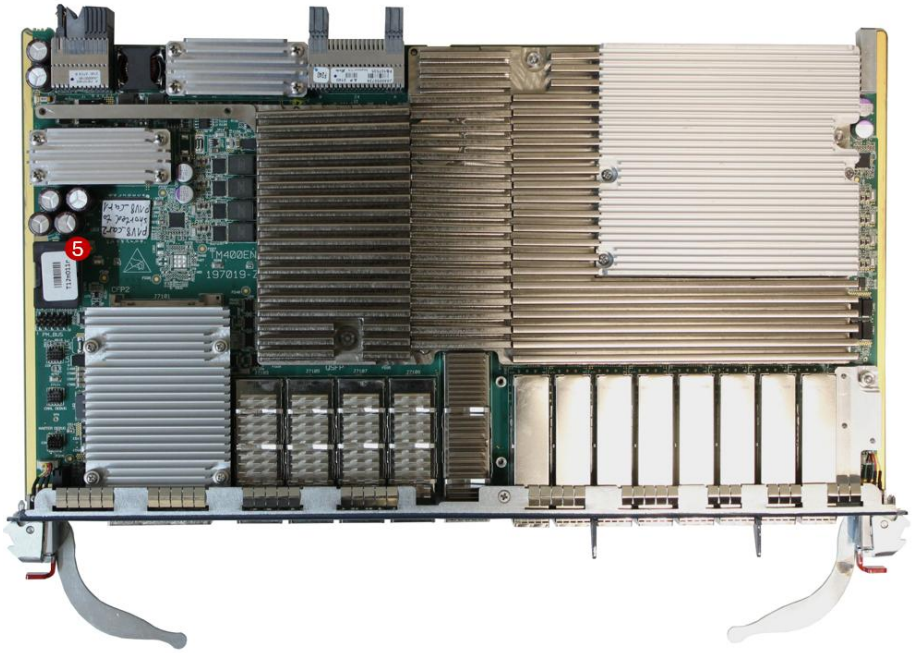
ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

3. Tamper seals are encoded with encoded characters and their inventory is carefully tracked by the CO. Additional tamper seals can be ordered (part# X93617) separately from Ribbon Communications if necessary (e.g. if after a visual inspection the CO detects that any tamper seal is damaged).

The CO is responsible for performing a physical inspection of the module to ensure the module has not suffered any attempt of tampering.

The following pictures cover the physical-security & tamper-evidence features of the module.





ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.



Figure 7: Tamper Evidence Seals Applied Across Critical Areas of the module



Figure 8: Metallic Tamper Shield Sealed and Mated with the PCB (front)

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.



Figure 9: Front Panel Before Installing Pick Resistant Lock

7.2 EFP/EFT Information

Temp/Voltage Type	Temperature or Voltage	EFP or EFT	Result
LowTemperature	-30°C	EFP	Shutdown
HighTemperature	50°C	EFP	Shutdown
LowVoltage	42.0V (DC)	EFP	Shutdown
HighVoltage	73.0V (DC)	EFP	Shutdown

Table 15: EFP/EFT Information

The module provides protection against environmental failure. It monitors the supplied voltage and the operating temperature and compares the values with maximum and minimum limits.

Upon detection that one of the monitored parameters is outside the allowed range, the software immediately automatically powers down the module, thus preventing any customer-sensitive data from being sent out from it. Moreover, the module will output via the serial port and record in the error log a message specifying the reasoning to enter in Environmental Failure Protection state.

The module will try to power up again, and it will not be able to be operational again if the faulty condition (temperature or voltage is out of range) remains. The module will keep powering down and up again until the voltage and temperature are back to normal boundaries.

7.3 Hardness Testing Temperature Ranges

Temperature Type	Temperature
LowTemperature	-30°C
HighTemperature	50°C

Table 16: Hardness Testing Temperatures

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

8 Non-Invasive Security

According to section 6.2 of the [SP 800-140F] document, there is no requirement specified at the moment regarding the non-invasive security, therefore, FIPS 140-3 Non-invasive Security requirements are not applicable because the module is not designed to implement non-invasive attack mitigation techniques.

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

9 Sensitive Security Parameters Management

This section provides details of the SSPs managed by the module during its life cycle. The module is able to generate keys using an approved CTR-DRBG, moreover, it supports SSP entry and is able to carry out key establishment during normal operation.

Additionally, it is able to zeroize ephemeral and temporal SSPs when they are no longer needed and implements a specific service of zeroization to zeroize all the unprotected SSPs stored within the module.

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
RAM (from TCPM-2)	Most CSPs and PSPs are stored in plaintext here	Dynamic
TOD-RAM	It is a battery Backed-Up RAM that is utilized by the module to store CSPs and to store a flag for tamper indication	Dynamic
CPLD flash memory	Flash memory placed into the CPLD component	Static
CPU_ROM	ROM memory placed into the TCPM-2 CPU	Static
SPI boot flash	It is an SPI flash memory attached to the Digi-G5 module	Static
SPI flash memory	Is an SPI flash memory controlled by the CPLD that incorporates several data protection methods	Static
Shadow file	File that contains the user_pwds related to the user operators	Static

Table 17: Storage Areas

The module stores most CSPs and PSPs in RAM in plaintext, except:

- The KEK is stored in plaintext in the TOD-RAM (a battery-backed-up RAM).
- The CO_pwd (plaintext), M_Public and M_Private (encrypted using KEK and AES-CBC-256) are stored in CPLD flash memory.
- The Boot_public is stored in embedded CPU_ROM in plaintext.
- The HEK and HDK are stored in the SPI boot flash attached to the Digi-G5 in plaintext.
- The M_cert and CA_cert are stored in plaintext in SPI flash memory.

The CO is the only operator allowed by the module to access or modify some SSPs (as M_private, M_public, M_cert, and CA_cert) stored in the module. The user operator can only modify his authentication password (User_pwd).

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
M_Private and M_Public (RSA private Key)	Loaded from the exterior by the CO in encrypted form via SSH session during the module installation and initialization. Note: No assurance of minimum security of SSPs (e.g., keys, bit strings) that are externally loaded, or of SSPs established with externally loaded SSPs	CPLD flash memory	Encrypted	Manual	Electronic	SSH traffic encryption

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
M_cert (X.509 cert)	Loaded from the exterior by the CO in encrypted form via SSH session. Note: No assurance of minimum security of SSPs (e.g., keys, bit strings) that are externally loaded, or of SSPs established with externally loaded SSPs	SPI flash memory	Encrypted	Manual	Electronic	SSH traffic encryption
CA_cert (X.509 cert)	Loaded from the exterior by the CO in encrypted form via SSH session. Note: No assurance of minimum security of SSPs (e.g., keys, bit strings) that are externally loaded, or of SSPs established with externally loaded SSPs	SPI flash memory	Encrypted	Manual	Electronic	SSH traffic encryption
Boot_Public	Integrated to Boot code image that is burnt into CPU_ROM during the manufacturing process	CPU_ROM	Plaintext	Manual	Electronic	
CO_pwd	Entered by the CO during the installation/initialization of the module or updated anytime by the CO, via the serial port console	CPLD flash memory	Plaintext	Manual	Electronic	
User_pwd	From System Card (RCP)	Shadow file	Plaintext	Automated	Electronic	SHA2-512 (A7386)
Output to the peer module	CPLD flash memory	Peer module as part of its associated module certificate M_Cert	Plaintext	Automated	Electronic	Peer module authentication
ECDH_Pub_K	RAM (from TCPM-2)	Either the peer module in case of key establishment for line-traffic encryption or the device	Plaintext	Automated	Electronic	KAS-ECC-SSC Sp800-56Ar3 (A7386)

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
		from which SSH session is established				

Table 18: SSP Input-Output Methods

The module supports the entry of CSPs such as the CO_pwd and the M_Private key during the secure installation and initialization process using the serial port with an attached cable to a PC.

Once the CO_pwd is set, the CO can log into the module through the serial port establishing an SSH secure channel to load the M_private key (in case it is loaded instead of generated into the module), therefore, the M_private key is loaded encrypted under the SSH secure channel.

These CSPs are required to configure the module to be able to operate in Approved mode.

Moreover, the module supports the input of PSPs such as M_cert and CA_cert certificates via the SSH secure channel as detailed above.

The CO_pwd is entered only via the serial port console with the cable mentioned above. It is checked for minimum length and usage of characters (according to the detailed in the Authentication Methods Table to comply with [SP 800-63B]) and must be repeated twice as security measure to be accepted by the module.

Finally, the module is only able to output the M_Public PSP and its associated certificate M_Cert in plaintext to perform the peer-to-peer authentication, however, it is not able to output any CSP.

9.3 SSP Zeroization Methods

The module supports several kinds of zeroization methods with different purposes. When one of the zeroization services is executed, the SSPs are overwritten with either ‘0’s or ‘1’s as detailed in the SSP Table 2.

The following table specifies the types of zeroization supported by the module:

Zeroization Method	Description	Rationale	Operator Initiation
Zeroization service	AES-256-CBC Key Encryption Key (KEK) and IV are overwritten in the TOD-RAM with all '0's. Encrypted RSA private key "M_Private" in the CPLD flash memory is overwritten with all '1's. Certificates "M_Cert" (containing RSA public key "M_Public") and "CA_Cert" in the SPI flash memory are overwritten with all '1's. Shadow file containing the user passwords is deleted from the file system. During the execution of the service, the security LED blinks in red with the pattern 1 sec on/1 sec off, and, once completed the zeroization is completed, the operation is logged in the log file. The security LED blinks in orange with the 2.5 sec on/2.5 sec off pattern and the message specified in the table of Approved Services is output via the CO Shell	Zeroization of all the CSPs stored into the module except the CO_pwd because it will cause the module to result inoperable	Zeroization request by the CO using the "zeroize" command
Partial zeroization	In the case of reset/reboot, all the HEKs and HDKs (for all encrypted service channels) are removed from the SPI boot flash attached to the Digi-G5, and all temporary SSPs that might reside in RAM (potentially in the middle of channel establishments) are also wiped off. HEKs and HEKs	Traffic encryption keys are zeroized, requiring to be re-negotiated after to allow the module encrypting or	Reset/Reboot

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Zeroization Method	Description	Rationale	Operator Initiation
	for the services are required to be re-renegotiated with peers to carry out the traffic encryption through the client and line ports	decrypting traffic via de line-port	
Tamper response	In case of tampering during operational time (not when the module is not powered), the KEK and CO_pwd are zeroized as detailed in the "7 Physical Security" section, and the event is reported in the error log. This causes the M_private and M_public to be permanently lost since they are encrypted with KEK. In this case, the security LED blinks according to the indicated in the table of Error States	Those CSPs are zeroized not to be available to any attacker. Moreover, the module results inoperable requiring to be repaired at Ribbon facilities	Tamper Event
Zeroization after use	The SSPs stored in RAM are zeorized after their usage	Zeroization of all CSPs stored in RAM	

Table 19: SSP Zeroization Methods

9.4 SSPs

The following tables expose the list of SSPs managed by the module:

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
HEK	AES key established with the peer for encrypting the traffic stream arriving from a client port before it is sent out on the line port	256 - 256	Symmetric Key - CSP		KAS-ECC (KBKDF)	Traffic Encryption and Decryption
HDK	AES key established with the peer for decrypting the traffic stream arriving on the line port before it is sent out on a client port	256 - 256	Symmetric Key - CSP		KAS-ECC (KBKDF)	Traffic Encryption and Decryption
M_Private	Module's RSA Private key associated with the certificate M_Cert that is used to perform peer authentication	>=2048 - >=112	Private key - CSP	RSA module's key pair generation		Peer module authentication
M_Public	Module's RSA Public key, included in the	>=2048 - >=112	Public key - PSP	RSA module's key pair generation		Peer module authentication

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	module certificate M_Cert that is used to perform peer authentication			Computed from M_Private upon SW request using an OpenSSL call		
KEK	AES key is used to encrypt the M_Private key before storing it in the module. It is also used internally for decrypting the M_Private key when required	256 - 256	Symmetric Key - CSP	CKG		SSPs encryption
M_cert	This is module's X.509 certificate issued to a specific module by a CA. it is used for performing peer authentication.	>=2048 - >=112	Authentication - PSP			Peer module authentication
CA_cert	This is the Root-CA certificate used to authenticate the certificates sent by other remote peer modules	>=2048 - >=112	Authentication - PSP			Peer module authentication
Boot_Public	This public key is used to perform the signature verification of the Kernel OS SW image	4096 - 140	RSA Key - PSP			Firmware integrity verification
CO_pwd	This CSP is used to authenticate the CO in the module. It is required in order to perform secure installation /initialization of the module and execute CO services	64 to 160 - 64 to 160	Password - CSP			

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
User_pwd	This CSP is used to authenticate the user in the module. It is required to execute user services per user class	64 - 64	Password - CSP			KAS-ECC (SSH)
DRBG Seed	Random Number Generation seed	384 - 384	Seed - CSP	Entropy collected from entropy source at instantiation		RSA module's key pair generation KAS-ECC (KBKDF) KAS-ECC (SSH) CKG
DRBG Internal Value	Random Number Generation internal value (V)	128 - 128	Internal Value - CSP	Counter DRBG (A7386)		RSA module's key pair generation KAS-ECC (KBKDF) KAS-ECC (SSH) CKG
DRBG Key	Internal DRBG key value	256 - 256	Symmetric key - CSP	Counter DRBG (A7386)		RSA module's key pair generation KAS-ECC (KBKDF) KAS-ECC (SSH) CKG
KH_Key	HMAC key entered into the HMAC function (Extractor) together with KBKDF_MK (ECDH shared secret), to provide a key value to the KDF function (Expander) that will derive the session keys (HEK and HDK)	256 - 256	Symmetric key - CSP	Derived from [Ni - nonce locally generated] and [Nr peer - nonce generated by the peer] for Tx direction and from [Ni peer - nonce generated by the peer] and [Nr - nonce locally generated] for Rx direction		KAS-ECC (KBKDF)
KBKDF_MK	This key is the ECDH shared secret that serves as an	256 - 256	Shared secret - CSP	KAS-ECC (KBKDF)		KAS-ECC (KBKDF)

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	Input to the HMAC function (Extractor) together with the KH_Key, to provide a key value to the KDF function (Expander) that will derive the session keys (HEK and HDK)					
ECDH_Priv_K	Private component of EC_Diffie Hellman Key Agreement with curves (P-256, P-384 and P-521)	256, 384, 521 - 128, 192, 256	Private key - CSP	Counter DRBG (A7386)		KAS-ECC (KBKDF) KAS-ECC (SSH)
ECDH_Pub_K	Public component of EC_Diffie Hellman Key Agreement with curves (P-256, P-384 and P-521)	256, 384, 521 - 128, 192, 256	Public key - PSP	Counter DRBG (A7386)		KAS-ECC (KBKDF) KAS-ECC (SSH)
SSH_KDF_K	This key is the ECDH shared secret that serves as an Input to the hash function used as PRF to derive the key in an SSH connection	256 - 256	Shared secret - CSP	KAS-ECC (SSH)		KAS-ECC (SSH)
SSH_K	This key is used to encrypt the data through the serial port when the SSH session is established once the CO or user is logged into the module	128, 192, 256 - 128, 192, 256	Symmetric key - CSP		KAS-ECC (SSH)	SSH traffic encryption

Table 20: SSP Table 1

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
HEK		SPI boot flash:Plaintext	Until Key Rotation or reset/reboot	Partial zeroization	KBKDF_MK:Derived From KH_Key:Derived From
HDK		SPI boot flash:Plaintext	Until Key Rotation or reset/reboot	Partial zeroization	KBKDF_MK:Derived From KH_Key:Derived From
M_Private	M_Private and M_Public (RSA private Key)	CPLD flash memory:Encrypted	Until zeroization is requested	Zeroization service	M_Public:Paired With M_cert:Paired With
M_Public	M_Private and M_Public (RSA private Key) Output to the peer module	CPLD flash memory:Encrypted	Until zeroization is requested	Zeroization service	M_Private:Paired With M_cert:Paired With
KEK		TOD-RAM:Plaintext	Until zeroization is requested	Zeroization service Tamper response	M_Private:Encrypts
M_cert	Output to the peer module M_cert (X.509 cert)	SPI flash memory:Plaintext	Until zeroization is requested	Zeroization service	M_Public:Paired With CA_cert:Paired With
CA_cert	CA_cert (X.509 cert)	SPI flash memory:Plaintext	Until zeroization is requested	Zeroization service	M_cert:Paired With
Boot_Public	Boot_Public	CPU_ROM:Plaintext	N/A	N/A	
CO_pwd	CO_pwd	CPLD flash memory:Plaintext	Until Tamper Event	Tamper response	
User_pwd	User_pwd	Shadow file:Encrypted	Until zeroization is requested or until the module's restart.	Zeroization service	
DRBG Seed		RAM (from TCPM-2):Plaintext	Until it is used	Zeroization after use	
DRBG Internal Value		RAM (from TCPM-2):Plaintext	Until it is used	Zeroization after use	
DRBG Key		RAM (from TCPM-2):Plaintext	Until it is used	Zeroization after use	
KH_Key		RAM (from TCPM-2):Plaintext	Until it is used, a tamper is detected or the module is reseated.	Zeroization after use	
KBKDF_MK		RAM (from TCPM-2):Plaintext	Until it is used, a tamper is detected or the	Zeroization after use	

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
			module is reseated.		
ECDH_Priv_K		RAM (from TCPM-2):Plaintext	Until it is used, a tamper is detected or the module is reseated.	Zeroization after use	ECDH_Pub_K:Paired With
ECDH_Pub_K	ECDH_Pub_K	RAM (from TCPM-2):Plaintext	Until it is used, a tamper is detected or the module is reseated.	Zeroization after use	ECDH_Priv_K:Paired With
SSH_KDF_K		RAM (from TCPM-2):Plaintext	Until it is used, a tamper is detected or the module is reseated.	Zeroization after use	
SSH_K		RAM (from TCPM-2):Plaintext	Until it is used, a tamper is detected or the module is reseated.	Zeroization after use	SSH_KDF_K:Derived From

Table 21: SSP Table 2

9.5 Transitions

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

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

10 Self-Tests

This section describes the pre-operational and conditional self-tests performed by the module to comply with the self-test requirements from FIPS 140-3. During the execution of self-tests, all data output interfaces are inhibited, therefore, no data is output from the data output interfaces.

In addition, in case of error during the self-tests, the module enters in error state (General error state, tamper-detection error state, or Low-Battery/PO-Tamper error state) requiring a power-cycling automatically executed by the System Card to force the execution of the pre-operational and conditional self-tests in order to recover the normal operation.

When the module enters in error state, the error is recorded in the error log and/or output via the serial port (for those cases in which the error log is not enabled because the software application is not running yet, the message is only output via the serial port).

Note: During the pre-operational self-tests, the module checks if a CO_pwd has already been configured into the module. In the negative case, the module enters the Missing CO-password state to force the CO to perform the initial configuration. Therefore, the Missing CO-password is not an error state although the verification of the existence of the CO_pwd is part of the critical function test performed during the pre-operational self-tests. Moreover, once the CO_pwd is configured for the first time, the module will never enter this state again.

10.1 Pre-Operational Self-Tests

The module executes a firmware and software integrity test, bypass test, and critical function test during pre-operational self-tests:

As the module is powered up, a set of firmware, software, and hardware tests are automatically launched. The module enters in error state (General error state, tamper-detection error state, or Low-Battery/Tamper error state) if there is a self-test failure at this stage.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
Critical Functions Test - Tamper test	Checks if there was a tamper event prior to the ongoing initialization	On-board tamper detection circuitry checks if a tamper event has occurred prior to initializing the module	Critical Function	If the test is passed with success the module executes the critical function tests called Power Failures or tampering test detailed in the row below. In case of failure, the module enters in tamper detection error state and the module's LEDs blink according to the table of Error States	Indicated below the table
Critical Functions Test - Power Failures or tampering test	Check for tamper event/low battery event	Check for power failures or tamper while the module was powered-off	Critical Function	If the test is passed with success the module executes the critical function tests called CO_pwd test. In case of failure, the module enters in Low-Battery/PO-	Indicated below the table

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
				Tamper error state and the module's LEDs blink according to the table of Error States	
Critical Functions Test - CO password test	Check if the CO_pwd is missing	The custom logic checks if there is a valid CO_pwd configured in the module	Critical Function	If the test is passed with success the module executes the Software/Firmware integrity test. In case of failure, the module enters in Missing CO-Password state and the module's LEDs blink according to the table of Error States	Indicated below the table
Software/Firmware integrity test	RSA PKCS v1.5 with 4096 modulus and SHA256 using Boot_Public key	Firmware integrity test based on Signature Verification	SW/FW Integrity	If the test is passed with success the module executes the critical function tests called H/W Encryption/Decryption verification detailed below. In case of failure, the module enters in General Error state	Signature verification to verify the firmware integrity. More details are provided below the table
Critical Functions Test - H/W Encryption/Decryption verification	Check the correct operativity of the encryption channels	H/W Encryption/Decryption verification.	Critical Function	If the test is passed with success the module executes the bypass test detailed below. . In case of failure, the module enters in General Error state	Indicated below the table
Bypass Test	Check the correct functioning of the Bypass functionality	Creating a bidirectional client channel with a local loopback in the line port	Bypass	If the test is passed with success the module starts the execution of the conditional self-tests. In case of failure, the module enters in General Error state	Indicated below the table

Table 22: Pre-Operational Self-Tests

Below are further details about the pre-operational self-test implemented in the module:

Critical Functions Test:

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

The module executes a pre-boot check as part of power-sequencing where the onboard CPU is held under reset. This test covers a set of tests performed by on-board custom hardware before the CPU reset is removed. Specifically, the following three critical function tests:

1. The on-board tamper detection circuitry checks if there was a tamper event prior to the ongoing initialization. In the case of tampering, the module enters in “tamper-detection error” and turns on the designated LEDs according to the Error States Table. In addition, a message indicating the tampering is output via the serial port. In case of tampering, the module must be sent back to Ribbon Communications facilities to be repaired.
2. The logic checks for power failures of the on-board battery or tampering while the module was previously not powered up. In the case any of them occurs, the module enters in “Low-Battery/PO-Tamper error” and the LEDs are configured according to the Error States Table and the message “Suspected tamper event/low battery event” is generated on the serial (console) port of the module. The CO must follow the corresponding documentation and inspect the module before giving consent to recover the normal operation from this condition.
3. The custom logic checks if there is a valid CO_pwd configured in the module. The module is shipped from the Ribbon Communications factory without CO_pwd . The CO must assign a valid password to the module before the initialization can proceed. The module enters in “Missing CO Password” state, and the LEDs are configured according to the Error States Table. If the password is missing the following message is output “Firmware password invalid/missing. Please enter new password” via the serial port. This is a special case that does not cause the module to enter in error state because its goal is to force the CO to configure a password as part of the initialization process. Therefore, the module resumes the normal operation once the CO sets the CO_pwd.

Note: The error messages are returned via the serial port instead of recorded in the error log because the s/w application is still not running at this point, and, therefore, the error log is still not available.

Apart from the tests described above that are executed during the boot, once the application is running, the following H/W Encryption/Decryption verification test is executed:

The correct operativity of the hardware encryption/decryption channels (that are used to process customer traffic at the client port’s rate) is checked next. These channels can be programmed for SSE (Single Shot Encryption), where a single frame containing test data can be encrypted/decrypted using the s/w supplied parameters. Outputs of encryption & decryption blocks are matched against the known answers stored in the software application.

This test is performed for all possible Encryption Machines in the Digi-G5 device that may be used: (4 internal Slices) * (10 Encryption Channels per slice) * (4 Secure Engines: Auth./Enc. for Rx/Tx) = 160 SSE (Single Shot Encryption) tests. Therefore, this critical function can be considered as a KAT for the algorithms implemented in Digi-G5 component (AES-GMAC and AES-CTR, Cert. #C1410).

In case of failure, the module enters in error state (General error state), reflecting it with the LEDs configured according to the Error States Table and recording the following error “Single Shot Encryption test failed. Shutting down..." in the error log. Once the module enters in “General error state” the System Card causes the power-cycling of the module to recover the normal operation in case of executing the pre-operational and conditional self-tests with success.

Software/Firmware Integrity Check Algorithms Test:

Boot-ROM is secured under the tamper shield. If the pre-boot phase passes, it implies that the boot ROM is secure. The boot-ROM application performs the following tests:

- Boot-ROM algorithms self-test:

  Boot-ROM is responsible for performing the conditional self-tests detailed in section “10.2 Conditional Self-test” related to the execution of RSA PKCS v1.5 signature verification with 4096 bits modulus and SHA256 message digest KATs.

If these tests are passed successfully, the Boot-ROM can fetch the SW application bundle from the System Card (RCP) and test its integrity and authenticity using those algorithms.

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

- S/W & F/W Integrity and authenticity test:

  After successfully running the conditional self-tests detailed above, the boot-ROM code fetches a file containing a software bundle from the System card. This file is a software bundle that contains the operating system (OS), the s/w application, and various other supporting components such as FPGA images. The file is digitally signed by Ribbon Communications' secure build servers at the time of its creation.

  The boot-ROM has the necessary, in-built RSA-public (Boot_public) to verify the digital signature of the software bundle performing the firmware integrity test. This public key corresponds to the private key of the secure signing server at Ribbon Communications.

  Successful signature verification of the software bundle implies that the bundle is authentic (generated by Ribbon Communications) and free of tampering. Therefore, a single signature verification proves the authenticity of all the components of the software bundle. In case of failure, the module enters in error state (General error state), reflecting it with the LEDs configured according to the Error States Table, and, taking into account that the software application is not running at this point and that the error log is not available yet, the module outputs the following message "Verifying integrity ... sha256,rsa4096:tcpm-u-boot- error!" via the serial port. Moreover, the System Card causes the power cycling of the module to recover the normal operation in case of executing the pre-operational and conditional self-tests with success.

  After signature verification, the Boot-ROM extracts various software components from the bundle loads these in System RAM, and then transfers the execution flow to the operating system that's loaded in System RAM.

The ROM propagates the 'chain-of-trust' to the OS, which then transfers it to the s/w application that runs as a user process of the OS. The s/w application (upon successful initialization) can then report to the management plane (i.e., System card) that it's running.

Bypass Test:

After the application executes the H/W Encryption/Decryption verification test with success, it performs a bypass capability test. This test is performed by creating a bidirectional client channel with a local loopback in the line port, sending a known pattern of data and monitoring how it is received back. The encryption and decryption on this channel are enabled and disabled, and the resultant synchronization of the data is compared with the expected due to different configurations of the two directions at each stage:

1. Configuring a user channel for 10GbE, bidirectional, non-encrypted
2. Performing a local loopback on the line port
3. Configuring an input traffic from an internal PRBS generator
4. Enabling encryption and decryption (full encryption trail)
5. Verifying data is received synchronized and error-free (bypass disabled, encrypted traffic is running)
6. Disabling decryption and verifying no sync
7. Disabling encryption and verifying data is received synchronized and error-free (bypass enabled, unencrypted traffic is running)

In case of failure during the bypass test, the module enters in error state (General error state) and it will be reflected with the LEDs configured according to the Error States Table and records the following error "Bypass Self-Test failed. Shutting down…" in the error log. Moreover, the System Card causes the power cycling the module to recover the normal operation in case of executing the pre-operational and conditional self-tests with success.

10.2 Conditional Self-Tests

The Conditional Self-Tests are detailed in the table below.

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
RSA SigVer (FIPS186-5) (A7385)	RSA with modulus 2048 and 4096 bits	KAT	CAST	In case of success the module executes the firmware integrity test. In case of failure, the module enters in General Error state	RSA signature verification	Prior to executing the firmware integrity test, the Boot-ROM execute this KAT required to perform the firmware integrity signature verification
SHA2-256 (A7385)	SHA256	KAT	CAST	In case of success, the module continues with the execution of CAST. Otherwise, the module enters in General Error state	SHA 256 verification	Prior to execute the firmware integrity test, the Boot-ROM execute this KAT required to perform the firmware integrity signature verification
HMAC-SHA2-224 (A7386)	HMAC-SHA224	KAT	CAST	In case of success, the module continues with the execution of CAST. Otherwise, the module enters in General Error state	HMAC verification	This test is executed in a group of tests after the module executes all the pre-operational self-tests and enters in conditional self-tests for the first time
HMAC-SHA2-256 (A7386)	HMAC-SHA256	KAT	CAST	In case of success, the module continues with the execution of CAST. Otherwise, the module enters in General Error state	HMAC verification	This test is executed in a group of tests after the module executes all the pre-operational self-tests and enters in conditional self-tests for the first time
HMAC-SHA2-384 (A7386)	HMAC-SHA384	KAT	CAST	In case of success, the module	HMAC verification	This test is executed in a group of tests

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				continues with the execution of CAST. Otherwise, the module enters in General Error state		after the module executes all the pre-operational self-tests and enters in conditional self-tests for the first time
HMAC-SHA2-512 (A7386)	HMAC-SHA512	KAT	CAST	In case of success, the module continues with the execution of CAST. Otherwise, the module enters in General Error state	HMAC verification	This test is executed in a group of tests after the module executes all the pre-operational self-tests and enters in conditional self-tests for the first time
AES-GCM Encryption KAT	AES-256-GCM	KAT	CAST	In case of success, the module continues with the execution of CAST. Otherwise, the module enters in General Error state	AES GCM encryption KAT	This test is executed in a group of tests after the module executes all the pre-operational self-tests and enters in conditional self-tests for the first time
AES-GCM Decryption KAT	AES-256-GCM	KAT	CAST	In case of success, the module continues with the execution of CAST. Otherwise, the module enters in General Error state	AES GCM decryption KAT	This test is executed in a group of tests after the module executes all the pre-operational self-tests and enters in conditional self-tests for the first time
AES-CBC Encryption KAT	AES-256-CBC	KAT	CAST	In case of success, the module continues with the execution	AES CBC encryption KAT	This test is executed in a group of tests after the module

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				of CAST. Otherwise, the module enters in General Error state		executes all the pre-operational self-tests and enters in conditional self-tests for the first time
AES-CBC Decryption KAT	AES-256-CBC	KAT	CAST	In case of success, the module continues with the execution of CAST. Otherwise, the module enters in General Error state	AES CBC decryption KAT	This test is executed in a group of tests after the module executes all the pre-operational self-tests and enters in conditional self-tests for the first time
KAS-ECC-SSC Sp800-56Ar3 (A7386)	ECDH with the P-256 curve	KAT	CAST	In case of success, the module continues with the execution of CAST. Otherwise, the module enters in General Error state	ECDH verification	This test is executed in a group of tests after the module executes all the pre-operational self-tests and enters in conditional self-tests for the first time
KDF SP800-108 (A7384)	KBKDF counter mode with HMAC-SHA256	KAT	CAST	In case of success, the module continues with the execution of CAST. Otherwise, the module enters in General Error state	KBKDF verification	This test is executed in a group of tests after the module executes all the pre-operational self-tests and enters in conditional self-tests for the first time
RSA SigGen (FIPS186-5) (A7386)	RSA with modulus (2048, 3072, 4096, 8192)	KAT	CAST	In case of success, the module continues with the execution of CAST. Otherwise, the	RSA signature generation	This test is executed in a group of tests after the module executes all the pre-operational

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				module enters in General Error state		self-tests and enters in conditional self-tests for the first time
RSA SigVer (FIPS186-5) (A7386)	RSA with modulus (2048, 3072, 4096, 8192)	KAT	CAST	In case of success, the module continues with the execution of CAST. Otherwise, the module enters in General Error state	RSA signature verification	This test is executed in a group of tests after the module executes all the pre-operational self-tests and enters in conditional self-tests for the first time
SHA2-224 (A7386)	SHA2-224	KAT	CAST	In case of success, the module continues with the execution of CAST. Otherwise, the module enters in General Error state	SHA verification	This test is executed in a group of tests after the module executes all the pre-operational self-tests and enters in conditional self-tests for the first time
SHA2-256 (A7386)	SHA2-256	KAT	CAST	In case of success, the module continues with the execution of CAST. Otherwise, the module enters in General Error state	SHA verification	This test is executed in a group of tests after the module executes all the pre-operational self-tests and enters in conditional self-tests for the first time
SHA2-384 (A7386)	SHA2-384	KAT	CAST	In case of success, the module continues with the execution of CAST. Otherwise, the module enters	SHA verification	This test is executed in a group of tests after the module executes all the pre-operational self-tests and enters in

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				in General Error state		conditional self-tests for the first time
SHA2-512 (A7386)	SHA2-512	KAT	CAST	In case of success, the module continues with the execution of CAST. Otherwise, the module enters in General Error state	SHA verification	This test is executed in a group of tests after the module executes all the pre-operational self-tests and enters in conditional self-tests for the first time
RCT	RCT	SP 800-90B Health tests; start-up and conditional	Critical Function	In case of success, the module continues with the execution of CAST. Otherwise, the module enters in General Error state	The Repetition Count Test is performed as specified in section 4.4.1 of the [SP 800-90B]	This test is executed in a group of tests after the module executes all the pre-operational self-tests and enters in conditional self-tests for the first time when the ENT is initialized for the first time
APT	APT	SP 800-90B Health tests; start-up and conditional	Critical Function	In case of success, the module continues with the execution of CAST. Otherwise, the module enters in General Error state	The Adaptative Proportion Test is performed as specified in section 4.4.2 of the [SP 800-90B]	This test is executed in a group of tests after the module executes all the pre-operational self-tests and enters in conditional self-tests for the first time when the ENT is initialized for the first time
Counter DRBG (A7386)	CTR_DRBG	KAT	CAST	In case of success, the module completes the execution of	Instantiate, generate, and reseed health tests for	This test is executed in a group of tests after the module

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				CAST. Otherwise, the module enters in General Error state	CTR_DRBG as stated in section 11.3 of the [SP 800-90Arev1]	executes all the pre-operational self-tests and enters in conditional self-tests for the first time when the CTR_DRBG is initialized for the first time
ECDSA KeyGen (FIPS186-5) (A7386)	P-256, P-384 and P-521	PCT	PCT	If it is executed with success the module generates ECDSA key pair as part of the ECDHE key establishment. Otherwise, the module enters in General Error state	ECDSA key pair generation with P-256, P-384 and P-521 curves	This test is executed when a new ECDSA key pair is generated as part of the ECDHE key establishment processes
RSA KeyGen (FIPS186-5) (A7386)	RSA with modulus (2048, 3072, 4096, 8192)	PCT	PCT	If it is executed with success the module executes the M_Public and M_Private keys correspondence test. Otherwise, the module enters in General Error state	RSA key pair signature generation and verification with modulus (2048, 3072, 4096, 8192)	This test is executed when a new RSA key pair is generated or loaded into the module
M_Public and M_Private keys correspondence test	The correspondence between M_private, M_public and M_cert is verified	PCT	Critical Function	In case of success, the module executes the M_Cert verification test. Otherwise, the module enters in General Error state	Additional information provided below the table	This test is executed when a new RSA key pair is generated or loaded into the module (after the execution of the RSA PCT)
M_Cert verification test	The integrity of the module's X.509 certificate is verified	Signature Verification	Critical Function	In case of success, the module executes the CA_Cert	Additional information provided below the table	This test is executed when a new RSA key pair is generated or

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				verification test. Otherwise, the module enters in General Error state		loaded into the module (after the execution of the M_Public and M_Private keys correspondence test)
CA_Cert verification test	The Cryptographic Authority's X.509 certificate CA_Cert is verified	Signature Verification	Critical Function	In case of success, the module goes to Ready state. Otherwise, the module enters in General Error state	Additional information provided below the table	This test is executed when a new RSA key pair is generated or loaded into the module (after the execution of the M_Cert verification test)

Table 23: Conditional Self-Tests

The module does not support manual key entry and firmware loading capabilities; therefore, the conditional self-tests encompass the cryptographic algorithm tests to verify the correct operativity of each cryptographic algorithm, and critical function tests. All tests are performed automatically without requiring user intervention, in order to make sure the module operates properly before service provisioning.

If the conditional self-tests are executed with success, the module will enter either in “SSP Entry or Generation” state if the module has not been properly initialized by the CO (the required SSPs to operate the cryptographic module have not been created or loaded into the cryptographic module) or in “Ready” state if the module has been properly initialized by the CO. In “Ready” state, the module is ready to execute whatever FIPS service when a command is received.

More details about the test can be found bellow:

Cryptographic Algorithms Test:

The algorithm self-tests are executed in two different stages:

- The first stage occurs during the Boot-ROM. The Boot-ROM implements RSA PKCS v1.5 signature verification and SHA256 message digest KATs (Known-Answer Tests) that are required to perform the firmware/software integrity check during the pre-operational self-tests. In case of failure, the module enters in error state (General error state) and it will be reflected with the LEDs configured according to the Error States Table and messages via the serial port (If this error occurs, the CO is responsible for collecting the logs and sending the module to repair in Ribbon facilities).

  Note: The error messages are returned via the serial port instead of being recorded in the error log because the s/w application is still not running at this point, and, therefore, the error log is still not available.

- The second stage occurs once the pre-operational self-tests have been passed with success. After executing the pre-operational self-tests, the ‘chain of trust’ is assured if the OS starts execution. The OS launches the proprietary embedded application as a user space process. The execution of KATs related to the cryptographic algorithms and critical tests defined in the section below are executed by the embedded application.

The list of KATs executed in this stage is detailed below:

- HMAC KAT for HMAC-SHA2-224, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512.

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

- AES-CBC-256 KAT for encryption and decryption operations.
- AES-GMC-256 KAT for authenticated encryption and decryption.
- AES-CBC-256 KAT for authenticated encryption and decryption.
- ECDH KAS-SSC KAT using the P-256 curve.
- KBKDF counter mode with HMAC-SHA256 KAT
- RSA KAT for signature generation and verification with modulus (2048, 3072, 4096, 8192).
- SHS KAT for SHA2-224, SHA2-256, SHA2-384 and SHA2-512 (these tests also cover SSH KDF KAT per Note 18 in FIPS 140-3 IG 10.3.A)
- ENT APT and RCT start-up health tests related to each entropy source as detailed in section 4 of the [SP 800-90B] document.
- CTR-DRBG KAT for instantiate, generate and reseed functions.

In case of failure in any of the implemented cryptographic algorithm self-tests, the module enters in error state (General error state) and it will be reflected with the LEDs configured according to the Error States Table and records the error related to the specific failed test in the error log. Moreover, the System Card causes the power cycling of the module to recover the normal operation in case of executing the pre-operational and conditional self-tests with success.

Pairwise Consistency Test:

The following pairwise consistency test will be executed in order to check the correct operativity of the module to perform signature generation/verification when the RSA key pairs are generated/loaded into the module and to check the correct generation of ECDSA key pairs required for ECDH key establishment:

- Pairwise consistency test for RSA key pair generation/loading and signature generation and verification with modulus (2048, 3072, 4096, 8192).
- Pairwise consistency test for ECDSA key pair generation (P-256, P-384 and P-521).

In case of failure in any of the implemented pairwise consistency tests, the module enters in error state (General error state) and it will be reflected with the LEDs configured according to the Error States Table and records the error "Pairwise Consistency Test failed. Shutting down..." in the error log. Moreover, the System Card causes the power cycling of the module to recover the normal operation in case of executing the pre-operational and conditional self-tests with success.

Continuous Entropy Health-Tests:

The module will execute the following continuous health-tests for the ENT:

- The Repetition Count Test (RCT) is performed as specified in section 4.4.1 of the [SP 800-90B].
- The Adaptative Proportion Test (ADPT) is performed as specified in section 4.4.2 of the [SP 800-90B].

In case of failure in any of the implemented continuous entropy health tests, the module enters in error state (General error state) and it will be reflected with the LEDs configured according to the Error States Table and records the error "IDQ Entropy health test failed. Shutting down..." in the error log. Moreover, the System Card causes the power cycling the module to recover the normal operation in case of executing the pre-operational and conditional self-tests with success.

Critical Functions Tests:

The application executes the following critical function tests:

The application executes the following critical function tests every time that an RSA key pair is either generated or loaded into the module. The purpose of these tests is to verify the correctness of the M_Private, M_Public, M_Cert, and CA_Cert before performing the PCT test prior to its first usage in order to avoid the module entering in error state in case the loaded keys contain any error or are corrupted:

1. M_Public and M_Private keys correspondence:

   The unique RSA key pair of the module comprises M_Private and M_Public. The private key M_Private is stored in an encrypted form onboard. It is read and decrypted using the KEK stored elsewhere inside the

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

module. The public key M_Public is included in the module's certificate M_Cert. Then the key pair is checked to verify their correspondence. If the check fails, the loaded SSPs are rejected, otherwise the module executes the M_Cert verification.

2. M_Cert verification:

   Once the M_Public and M_Private correspondence is checked. The integrity of the module's X.509 certificate is verified using the public key from Cryptographic Authority's X.509 certificate CA_Cert. If the check fails, the loaded SSPs are rejected, otherwise the module executes the M_Cert verification.

3. CA_Cert verification:

   Finally, the Cryptographic Authority's X.509 certificate CA_Cert is verified as detailed below:

   a. If it's a root certificate, its digital signature is verified using the public key in the certificate itself.
   b. If CA_Cert is not a root certificate, there will be a chain of certificates installed on the module. The entire chain is verified until the root certificate of that chain. Root certificates are always self-signed and verified using their own public key.

In the case the three tests are executed with success verifying the correctness of M_Public, M_Private, M_Cert, and CA_Cert, the module executes the RSA PCT prior to using the M_Private and M_Public keys for the first time.

A failure in any of these critical tests will cause the module to go again to "SSP Entry or Generation state" until a valid RSA key pair is generated or loaded into the module. When a valid RSA key pair is either generated or loaded into the module, it would mean that all these critical tests and the RSA PCT have been executed with success, and the module is ready to operate. In this case, the module does not enter in error state in case of failure because if the RSA key pair is not correct this will cause it to enter in error state infinitely. Therefore, in this case, the module goes to "SSP Entry or Generation state" to force the replacement of the module's RSA key pair and its correct configuration.

Bypass Tests:

Although the module may implement a bypass service to disable traffic encryption, it is not an exclusive bypass because it is applied independently to a specific communication channel. Moreover, the bypass cannot be active in those channels automatically because it is managed by the System-card (user operator). The module does not maintain internal information to govern which channels are working in bypass mode. In order to avoid a single point of failure when implementing a bypass service, when the user wishes to enable bypass via the management SW (EMS or Muse) interface he is prompted to approve the operation before it is executed.

Therefore, a conditional bypass test is not required to be performed when bypass capability is executed by the module.

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Critical Functions Test - Tamper test	On-board tamper detection circuitry checks if a tamper event has occurred prior to initializing the module	Critical Function	Module operational	Restart module or configured period between 1 to 5 years
Critical Functions Test - Power Failures or tampering test	Check for power failures or tamper while the module was powered-off	Critical Function	Module operational	Restart module or configured period between 1 to 5 years
Critical Functions Test - CO password test	The custom logic checks if there is a valid CO_pwd configured in the module	Critical Function	Module operational	Restart module or configured period between 1 to 5 years

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Software/Firmware integrity test	Firmware integrity test based on Signature Verification	SW/FW Integrity	Module operational	Restart module or configured period between 1 to 5 years
Critical Functions Test - H/W Encryption/Decryption verification	H/W Encryption/Decryption verification.	Critical Function	Module operational	Restart module or configured period between 1 to 5 years
Bypass Test	Creating a bidirectional client channel with a local loopback in the line port	Bypass	Module operational	Restart module or configured period between 1 to 5 years

Table 24: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
RSA SigVer (FIPS186-5) (A7385)	KAT	CAST	Module operational	Restart module or configured period between 1 to 5 years
SHA2-256 (A7385)	KAT	CAST	Module operational	Restart module or configured period between 1 to 5 years
HMAC-SHA2-224 (A7386)	KAT	CAST	Module operational	Restart module or configured period between 1 to 5 years
HMAC-SHA2-256 (A7386)	KAT	CAST	Module operational	Restart module or configured period between 1 to 5 years
HMAC-SHA2-384 (A7386)	KAT	CAST	Module operational	Restart module or configured period between 1 to 5 years
HMAC-SHA2-512 (A7386)	KAT	CAST	Module operational	Restart module or configured period between 1 to 5 years
AES-GCM Encryption KAT	KAT	CAST	Module operational	Restart module or configured period between 1 to 5 years
AES-GCM Decryption KAT	KAT	CAST	Module operational	Restart module or configured period between 1 to 5 years
AES-CBC Encryption KAT	KAT	CAST	Module operational	Restart module or configured period

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
				between 1 to 5 years
AES-CBC Decryption KAT	KAT	CAST	Module operational	Restart module or configured period between 1 to 5 years
KAS-ECC-SSC Sp800-56Ar3 (A7386)	KAT	CAST	Module operational	Restart module or configured period between 1 to 5 years
KDF SP800-108 (A7384)	KAT	CAST	Module operational	Restart module or configured period between 1 to 5 years
RSA SigGen (FIPS186-5) (A7386)	KAT	CAST	Module operational	Restart module or configured period between 1 to 5 years
RSA SigVer (FIPS186-5) (A7386)	KAT	CAST	Module operational	Restart module or configured period between 1 to 5 years
SHA2-224 (A7386)	KAT	CAST	Module operational	Restart module or configured period between 1 to 5 years
SHA2-256 (A7386)	KAT	CAST	Module operational	Restart module or configured period between 1 to 5 years
SHA2-384 (A7386)	KAT	CAST	Module operational	Restart module or configured period between 1 to 5 years
SHA2-512 (A7386)	KAT	CAST	Module operational	Restart module or configured period between 1 to 5 years
RCT	SP 800-90B Health tests; start-up and conditional	Critical Function	Module operational	Restart module or configured period between 1 to 5 years
APT	SP 800-90B Health tests; start-up and conditional	Critical Function	Module operational	Restart module or configured period between 1 to 5 years
Counter DRBG (A7386)	KAT	CAST	Module operational	Restart module or configured period between 1 to 5 years

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ECDSA KeyGen (FIPS186-5) (A7386)	PCT	PCT	Module operational	Any time that a ECDSA key is generated
RSA KeyGen (FIPS186-5) (A7386)	PCT	PCT	Module operational	Any time that a RSA key is generated or loaded
M_Public and M_Private keys correspondence test	PCT	Critical Function	Module operational	Any time that a RSA key is generated or loaded
M_Cert verification test	Signature Verification	Critical Function	Module operational	Any time that a RSA key is generated or loaded
CA_Cert verification test	Signature Verification	Critical Function	Module operational	Any time that a RSA key is generated or loaded

Table 25: Conditional Periodic Information

By default, the module executes periodic self-tests every 5 years. Moreover, it allows the user to configure the period of time between 1 to 5 years.

The module performs periodic self-tests by executing the pre-operational self-test and Conditional self-tests using software-driven power cycling when the configured period expires.

10.4 Error States

The table below shows the different causes that lead to the Error States and the status indicators reported.

Name	Description	Conditions	Recovery Method	Indicator
General Error State	A general error is detected	An error is detecting during self-test execution.	Power-cycling and execution of the self-test	The module prints the following message "STATE: GENERAL ERROR" in the error log and the serial port and it is automatically reset.
Tamper Detection Error state	A tamper event is detected	A tamper event occurred on the module	Non-recoverable	The Security LED is on Red Colour. The SW-U LED, IS LED and FAIL LED are off. Moreover, the module prints the following message "Main Tamper Cover Breach" in the serial port
Low-Battery/PO-Tamper error state	A low battery or tamper event is detected while the module is off	The battery of the module is close to running out	Power-cycling and execution of the self-test	The Security LED turns to red (2.5 seconds on/ 2.5 seconds off). The SW-U LED, IS LED and FAIL LED are off. Moreover, the module prints the following message "System Halted - Low battery or tamper event suspected" in the serial port

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Name	Description	Conditions	Recovery Method	Indicator
Missing CO-Password State	The CO_pwd is missing.	No CO_pwd is detected in the module	The CO must perform the initial configuration process	The Security LED turns 1.5 second on in green and 2.5 seconds on in RED. The SW-U LED, the IS LED and FAIL LED are off. Moreover, the module prints the following message "Firmware password invalid/missing" in the serial port
Env. Failure state	The module enters in this error when either the temperature and/or the input voltage are outside of the defined operation ranges	Temperature and/or voltage out of the operating rage	The module will keep on power cycling until the temperature and/or voltage are back to the values into the operating range	The module outputs the following message via the serial port:"STATE: Env. Failure". After that, it is automatically reset.

Table 26: Error States

Note: Although the module enters in Missing CO-Password State as a consequence of not having a CO_pwd configured, this is not an error state, but a state that requires to perform the initial configuration of the module. However, considering it is checked as critical function, it has been included in the table of errors obtained during execution of the self-tests.

10.5 Operator Initiation of Self-Tests

As stated above, the pre-operational self-tests can be performed on demand by resetting the module. Moreover, the module allows the operator to execute the software/firmware integrity check on demand by rebooting the module using the “run request chassis power reset” command.

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

Secure Distribution:

The module is shipped via certified courier service by Ribbon Communications, and it is shipped in a sealed box with a tamper and shipment identification label. Therefore, the CO will be able to notice if it is tampered with.

Integrity and Confidentiality Assurance:

When the module is received by the customer, the CO must verify the packaging as well as the integrity of tamper labels that are applied across factory-installed tamper covers. These factory's installed tamper labels provide the necessary protection against tamper.

If the tamper labels and module are intact and the module is operative, then, the Crypto officer can verify the module hardware and firmware version by sending the **"ver"** and **run show chassis inventory slot-<slot_number>** command through the serial interface after following the secure initialization process detailed in the following subsection.

If the crypto officer notices that the tamper labels from the shipping box and the module are damaged or that the enclosure has been tampered with, then, the module must not be initiated nor used to perform cryptographic operations. Ribbon Communications should be contacted to arrange the return of the module to Ribbon Communications facilities for inspection and any necessary reparation or exchange.

Installation and Initialization:

There are two different installation scenarios for a module specified in the following subsections.

New Module Arriving from Factory:

A new module is shipped without any CO_pwd. Once powered, initialization is halted for a module without a valid CO_pwd. The CO must configure a valid password through the module's serial port. Detailed instructions regarding this are shared with customers.

Re-Installation in Another Slot:

A previously installed/configured module may be relocated to another slot of the same or a different chassis if needed. However, the CO must verify the integrity of various tamper labels before doing so. Checking the factory-installed tamper seals is essential for FIPS level-3 compliance.

Previously configured CO_pwd will remain valid until it is explicitly modified by the CO.

Once a module is installed in a slot and CO_pwd is configured, the CO is advised to also apply tamper labels across the front panel that will help detect unauthorized removal of the board from its slot as well as any access to its serial ports. Front panel seals provide an additional layer of security even though the basic (tamper-indication) FIPS requirements are covered by the factory-installed tamper seals that are applied across the module's tamper covers.

Additional tamper labels can be ordered separately (part# X93617) as each seal can only be used once.

Initial Key Loading:

In addition to the physical installation & inspection of the module, the CO is also responsible for loading/generating the persistent CSPs. Subsequent to the CO_pwd configuration, the CO should generate the key-encryption key (KEK), either load or generate and encrypt the module's key pair (M_Private, M_Public), and load the corresponding module's certificate (M_Cert). Additionally, the CO must also load a CA certificate (CA_Cert). These parameters are stored within the module as detailed in SSP Table 2 various kinds of persistent memories of the module, which are all shielded by the tamper cover.

Subsequent to the above installation process, a module can operate in Approved mode, as it can securely establish encryption keys with remote peers and encrypt/decrypt client traffic using those keys. Configuration of services is handled by operators.

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Lockout Policy Configuration:

When the module is in approved mode, after following the installation and initialization steps, the CO must configure the lockout policy for the human operator by sending the following command through the CLI: **set system authentication login-fail-count 9**. This sets the number of failed login attempts in given interval to 9.

11.2 Administrator Guidance

The board will operate in Approved mode under normal operating conditions. There is no special configuration option required for this apart from the initial configuration to set a CO_pwd and the generation/loading of the module's RSA key pair. The board provides operational information to the System card that's indicative of working in Approved mode.

When a board is unable to operate to execute an approved service, the LEDs, the serial port (as detailed in section "2 Cryptographic Module Interfaces") and the controller card (e.g. 'show chassis alarms' CLI command) show the module state. The Security LED of a fully initialized board loaded with all SSPs shows solid green-colour. User documentation provides further details on interpreting other LED patterns corresponding to module internal operativity

There is a designed CO for each module. This person is responsible for the physical integrity of the module as well as in charge of performing secure installation and initialization of the module by generating/loading CSPs stored onboard.

Once the module is correctly initialized and configured, the CO can execute the services associated with him/her in the Approved Services Table.

11.3 Non-Administrator Guidance

The following covers instructions related to the configuration of the module, security events, and any assumptions related to the security of the module.

1. A properly configured module, loaded with CSPs can securely communicate with peer modules, without assuming the integrity of any intermediate network nodes (such as the System card). This is achieved through bi-directional verification of X.509 certificates between peers that are signed by a known & trusted CA.
2. The System card and the Ethernet interface between the System card and the module are trusted in so far as the service configuration/management is concerned. The System card sends proprietary messages to control services on the module and collects statistics and other operational data.
3. In this context, the management application (from the System card) or human operators (that are not CO) are considered "administrators".
4. It should however be noted that the administrators are not allowed to modify the CSPs loaded by the CO on the System card. The CO authenticates with the module using a separate CO_pwd (CO_pwd is stored in a protected persistent memory of the module).
5. Human operators and System-Card can execute their associated services in Approved Services Table once the module is initialized by the CO.

11.4 Design and Rules

When the module is installed and securely initialized as detailed in the section "11.1 Installation, Initialization, and Startup Procedures", it is initialized in Approved mode which is the only mode of operation that complies with the following rules:

1. The module is initialized in Approved mode of operation automatically after the self-tests are completed successfully and the initial key loading process has been performed.

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

2. The replacement or modification of the module by unauthorized users is prohibited.
3. The System Card's internal memory back-up battery should be replaced every two years.
4. Once the module is powered, the pre-operational self-tests are executed automatically without requiring any operator additional action to be executed.
5. The module does not implement a degraded mode of operation.
6. The module does not require a control output interface because it does not output control signals to control other modules.
7. All data output interfaces except status output interfaces will be inhibited when the module is performing self-test, key zeroization, key generation, or is in an error state.
8. The module does not support a maintenance interface or maintenance role.
9. The module provides bypass capability that is correctly tested during the pre-operational self-tests. Conditional self-tests are not required for the bypass as detailed in section "10.2 Conditional Self-test".
10. The module does not require a trusted channel because CSPs are entered in encrypted form into the module via the SSH channel.
11. The module does not implement firmware uploading or self-initiated capabilities.
12. The module provides identity-based authentication using passwords according to [SP 800-63B].
13. The module does not support manual key entry.
14. The module implements pre-operational self-tests to ensure the integrity of the firmware, critical functions, and bypass. The pre-operational self-test can be performed on demand by resetting the module.
15. The module implements conditional self-test to ensure the correctness of the implemented cryptographic algorithms, random number generation process, asymmetric key generation process, and critical function tests.
16. The crypto officer is in charge of uploading/generating the module CSPs (M_private and M_public) and X.509 certificates (CA_cert and M_Cert) during the module's initial key loading process.
17. If the module is in an error state, the cryptographic operativity of the module will be disabled.
18. The normal operation of the module can be resumed from an error state depending on the type of error:
    a. Tamper Detected: The module must be repaired at Ribbon Facilities.
    b. Low Battery/Tamper: The module must be checked by the CO in order to confirm that tamper labels are intact and that the battery is not degraded. In the affirmative case, the module recovers the normal operation after the CO confirmation.
    c. General error state: This error requires resetting the module in order to execute the pre-operational and conditional self-tests again. The module will resume the normal operation just if both self-tests are executed with success.
    d. Environmental Failure: The normal operation is resumed when the voltage and temperature are into the regular operation ranges.
19. The CO is responsible for performing periodic inspections of the module to ensure that the physical protections detailed in the "7 Physical Security" section are intact.

11.5 End of Life

When the customer no longer needs to use the module, it is highly recommended for them to sanitize it and then destroy it securely as follows:

Secure Sanitization:

The CO shall perform the following steps to sanitize the module:

1. Perform Zeroization service, as described in "4 Roles, Services, and Authentication"

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

2. Perform tamper: Pull the module out of the chassis, remove the tamper sticker, and open at least one tamper screw, then put the module back into its slot. Verify the module detects the tamper and does not initiate.

Secure Destruction:

The CO shall destroy the module after it is sanitized. Alternatively, the CO may choose to send the module back to Ribbon.

To securely destroy the module, the CO shall follow these recommendations:

1. Pull the module out of the chassis.
2. Unscrew and remove the module's heatsinks.
3. Remove the RAM battery.
4. Use any of the following methods to destroy the components on the board:
    a. Identify sensitive devices – all the larger IC devices on the board. These may be memory chips or storage devices and /or processors. Ensure that these are physically destroyed beyond recovery. Methods like drilling through the components or physically breaking them can be used.
    b. Use a secure shredder: If access to one is possible, consider using an industrial shredder designed for electronic components. This will make it extremely difficult for anyone to retrieve data or reassemble the module.
    c. Destroy circuitry: By using pliers, wire cutters, or a hammer to physically break and mangle the electronic circuitry on the module's PCB (Printed Circuit Board). Should be ensured that it's rendered unusable.
5. Dispose of remnants: The destroyed module and any remnants should be disposed of responsibly. According to the local waste disposal guidelines, which may involve recycling certain materials and sending hazardous waste to specialized facilities.
6. Document the process: Records of the destruction process, including photographs if necessary, should be kept in order to prove that you took reasonable steps to securely destroy the module.

Securely destructing an electric module should be done with safety and environmental concerns in mind. Safety should be always prioritized, follow local regulations for disposal, and take precautions to protect both yourself and the environment during the process taken.

11.6 Additional Information

Configuration Management:

The configuration management list is composed of the Configuration Items version control, change control, flaw remediation tracking, and source code revision which are managed by Ribbon Communications.

Best design practices are followed & various measures are taken to ensure sound firmware and hardware design of the module.

1. Ribbon Communications uses object-oriented software design practices and contemporary tools such as UML (Unified Modelling Language).
2. Ribbon Communications uses a well-known tool called Perforce (P4) for software configuration management (SCM) to ensure reproducibility of the firmware build considering it allows to perform file versioning, changes tracking, software development, releases management, defects tracking, bugs fixing and builds management. Similarly, a well-known open-source tool called reviewboard is used for the peer-code review process.
3. For programmable logic, Ribbon Communications uses Synchronicity for SCM.
4. Ribbon Communications uses a well-known document management system (DMS) called Sharepoint to document, review and modify designs.

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

5. Each key component of firmware implementation is peer-reviewed and unit-tested and it later goes through multiple rounds of features, stability, and regression testing for quality assurance purposes.
6. Similarly, the hardware (programmable logic as well as physical board) goes through several rounds of qualification before the release. The hardware meets US-FCC and other relevant standards from certification and statutory bodies in the countries where it is marketed.

Note: The Perforce, Reviewboard and Synchronity tools utilized for SCM and the Sharepoint utilized for DMS require user authentication to ensure that only authorized changes are made.

Traceability and Identification:

In a production environment, different physical components and firmware versions must be identifiable in order to correctly deploy a service that provides security as intended.

Hardware Identification:

All the FRU (Field Replaceable Unit) components contain Ribbon Communications labels, hardware revision numbers, and serial numbers visible on these parts. The module contains a PROM (Programmable Read-Only Memory) that stores this information which can also be retrieved remotely through the System card. This enables tracking of hardware parts. The software application from the System card exports revision information from each management application.

The module is comprised of 1 PCB and pluggable optical transceivers. The pluggable transceivers are outside the tamper covers. Additionally, the pluggable transceivers (XFP or SFP) on each port contain PROM data for their identification.

There are two tamper covers fastened to the board. These covers have tamper indicator seals placed at strategic points. Tamper seals have Ribbon Communications proprietary information in encoded form.

Firmware Traceability:

1. The boot-ROM image resident on the module has an associated revision that can be seen through an operational command executed on the System card. Connecting to the module via SSH and using the "**ver**" command.
2. There is also a revision associated with the s/w bundle operational on the module which can be accessed through an operational command. The specific command is **"show chassis card software <slot-number>"**.
3. The cryptographic components of the boot-ROM are versioned and tracked separately. This information can be retrieved through a boot-ROM CLI command called ***"GetBoardFipsMode"***.

Configuration Items Identification Method:

As required for FIPS 140-3 SL3, the versioning of the module's firmware and hardware and the document versioning are carried out according to the stated below in an automated way using the SCM and DMS configuration management tools listed above:

The software application version is assigned with the format 'X.Y.Z.W.+', where:

- X → It is a number indicating Major Version
- Y → It is a number indicating Minor Version
- Z → It is a number indicating Mini Minor Version
- W → It is a number indicating Pico Minor Version
- + → indicates it as a frozen version

The CPLD firmware version is assigned with the format 'XXYY', where:

- XX → It is a two-capital-letter indicator which can be one of the following:
    - 'EA' – is a released version
    - 'DB' – is a debug version
- YY → It is a two-digit number indicating the version ('04' is the 4th version)

The Boot ROM Cryptographic Components version is assigned with the format 'X.Y.Z.+', where:

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

- X → It is a number indicating Major Version
- Y → It is a number indicating Minor Version
- Z → It is a number indicating Mini Minor Version
- + → indicates it as a frozen version

The hardware version is assigned with the following format 'X.YY' where:

- X → It is a capital letter, indicating the PCB version ('D' is the 4th version).
- YY → It is a two-digit indicating the BOM version ('00' is the 1st version).

The documentation is versioned with the following format TM400ENB_name_v.X.Y where:

- TM400ENB → It is the module version.
- Name → It is the name of the document.
- X → It is a number indicating Major Version
- Y → It is a number indicating Minor Version

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

12 Mitigation of Other Attacks

The module is not designed to mitigate other attacks which are outside of the scope of the FIPS 140-3 standard.

ECI Telecom Ltd / Ribbon communications Operating company, Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.