VT iDirect, Inc.

Secure Satellite Broadband Solutions

Module Names: Evolution e8350-FIPSL2 Satellite Router Board [1], iConnex e800-FIPSL2 Satellite Router Board [2], iConnex e850MP-FIPSL2 Satellite Router Board [3], Evolution eM1D1-FIPSL2 Line Card [4], and Evolution eM0DM-FIPSL2 Line Card [5]

Firmware Versions: iDX versions 3.3.2.5 and 3.4.3.5

Hardware Versions: E0000051-0005 [1], E0001340-0001 [2], E0000731-0004 [3], E0001306-0001 [4], and E0001306-0002 [5]

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 2
Document Version: 1.4

Prepared for:

VT iDirect, Inc.
13861 Sunrise Valley Drive, Suite 300
Herndon, VA 20171
United States of America

Phone: +1 (866) 345-0983
http://www.idirect.net

Prepared by:

Corsec Security, Inc.
13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

Phone: +1 (703) 267-6050
http://www.corsec.com

Table of Contents

Table of Figures

List of Tables

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the following cryptographic modules from VT iDirect, Inc.:

- Evolution e8350™-FIPSL2 Satellite Router Board (Part # E0000051-0005)
- iConnex e800™-FIPSL2 Satellite Router Board (Part # E0001340-0001)
- iConnex e850MP™-FIPSL2 Satellite Router Board (Part # E0000731-0004)
- Evolution eM1D1™-FIPSL2 Line Card (Part # E0001306-0001)
- Evolution eM0DM™-FIPSL2 Line Card (Part # E0001306-0002)

The devices listed above were tested and validated running the following versions of firmware:

- iDX 3.3.2.5
- iDX 3.4.3.5

This Security Policy describes how the modules listed above meet the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S. and Canadian Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) and the Communications Security Establishment (CSE) Cryptographic Module Validation Program (CMVP) website at http://csrc.nist.gov/groups/STM/cmvp.

This document also describes how to run the modules in a secure FIPS-Approved mode of operation. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the modules. The Evolution e8350-FIPSL2 Satellite Router Board, iConnex e800-FIPSL2 Satellite Router Board, iConnex e850MP-FIPSL2 Satellite Router Board, Evolution eM1D1-FIPSL2 Line Card, and Evolution eM0DM-FIPSL2 Line Card are collectively referred to in this document as Secure Satellite Broadband Solutions, cryptographic modules, or modules.

1.2 References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The VT iDirect website (http://www.idirect.net) contains information on the full line of products from VT iDirect.
- The CMVP website (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm) contains contact information for individuals to answer technical or sales-related questions for the module.

1.3 Document Organization

The Security Policy document is organized into two (2) primary sections. Section 2 provides an overview of the validated modules. This includes a general description of the capabilities and the use of cryptography, as well as a presentation of the validation level achieved in each applicable functional areas of the FIPS standard. It also provides high-level descriptions of how the modules meet FIPS requirements in each functional area. Section 3 documents the guidance needed for the secure use of the module, including initial setup instructions and management methods and policies.

2 Secure Satellite Broadband Solutions

2.1 Overview

VT iDirect's satellite-based IP[1] communications technology enables constant connectivity for voice, video, and data applications in any environment. VT iDirect has developed the leading TRANSEC-compliant bandwidth-efficient satellite platforms for government and military communications. The Secure Satellite Broadband Solutions have uses across a wide range of applications, including maritime connectivity, aeronautical connectivity, military defense, and emergency relief.

VT iDirect Secure Satellite Broadband Solutions support a Time Division Multiple Access (TDMA) upstream carrier and DVB-S2[2] downstream carrier. The VT iDirect TDMA network is optimized for satellite transmissions, obtaining the maximum performance out of satellite bandwidth. The system is fully integrated with VT iDirect's Network Management System that provides configuration and monitoring functions. The VT iDirect network components consist of the Network Management Server, a Protocol Processor, a Hub Line Card, and the Ethernet switch with remote modem. In a star topology, the Protocol Processor acts as the central network controller, the Hub Line Card is responsible for the hub side modulation and demodulation (modem) functions, and the remote modem provides modem functionalities along with the Ethernet switch. A common deployment of the VT iDirect network components is shown in Figure 1 below. The following acronyms are used in Figure 1 and are previously undefined:

- BUC – Block Upconverter
- LNB – Low-noise Block Downconverter

[1] IP – Internet Protocol
[2] DVB-S2 – Digital Video Broadcast - Satellite - Second Generation

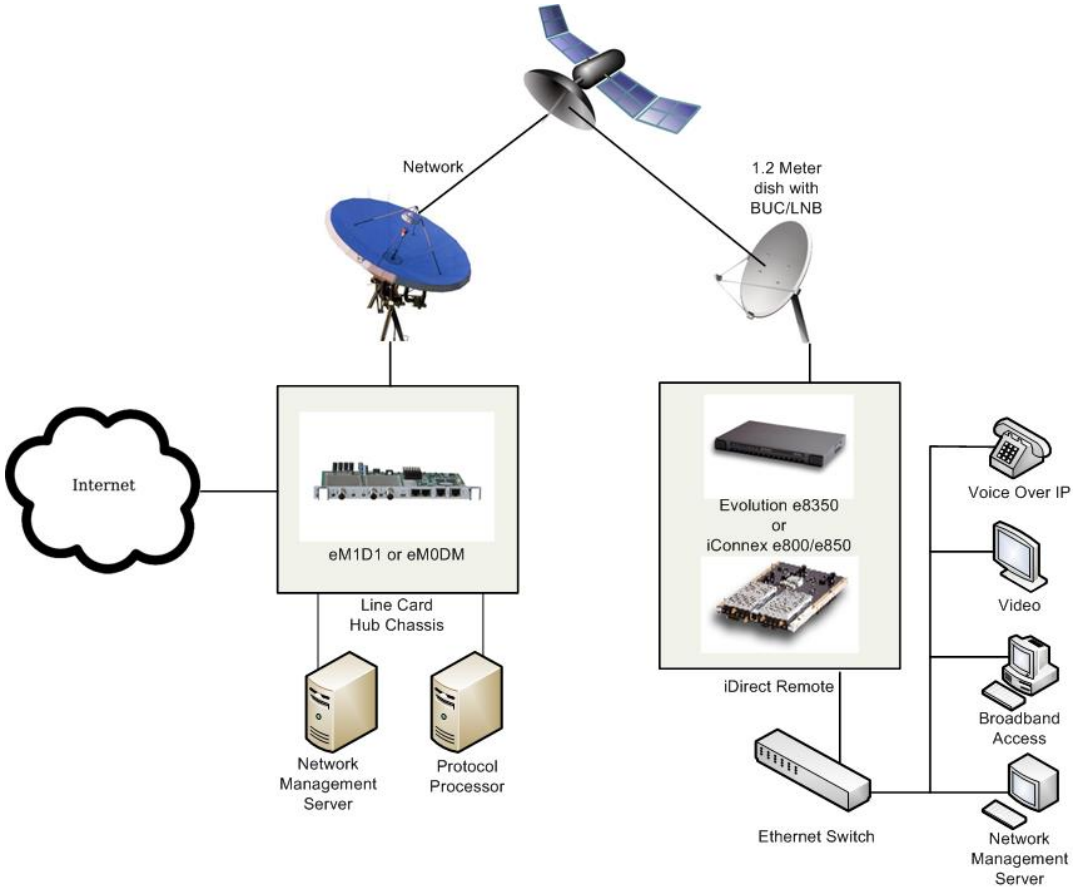

Figure 1 – VT iDirect Network Deployment

VT iDirect's hardware modules offer the Transmission Security (TRANSEC) feature that encrypts all Data Link Layer traffic including all control and management data flowing between the ULC[3] and the Remote modem using the Advanced Encryption Standard (AES). VT iDirect achieves full TRANSEC compliance by presenting to an adversary eavesdropping on the RF[4] link a continual stream of fixed-sized, strongly-encrypted traffic segments, the frequencies of which do not vary with network activity. All network messages, including those that control the admission of a remote terminal into the TRANSEC network, are encrypted and their original size is hidden. The content and size of all user traffic (Layer 3 and above), as well as all network link layer traffic (Layer 2), is completely indistinguishable from an adversary's perspective. In addition, no higher-layer information can be ascertained by monitoring the physical layer (Layer 1) signal. VT iDirect TRANSEC includes a remote-to-hub and a hub-to-remote authentication protocol, based on X.509 certificates, designed to prevent man-in-the-middle attacks. This authentication mechanism prevents an adversary's remote from joining a VT iDirect TRANSEC network. In a similar manner, it prevents an adversary from coercing a TRANSEC remote into joining the adversary's network.

TRANSEC is managed by the module firmware. A key set is created for each TRANSEC controller and all participants in that controller's Star network share an exclusive key set. Encryption of data occurs in FPGA[5] firmware. TRANSEC encrypts all data in Layer 2, including High-Level Data Link Control (HDLC) packets. Multicast and broadcast data is also encrypted. Since the key set is shared among the

[3] ULC – Universal Line Card
[4] RF – Radio Frequency
[5] FPGA – Field Programmable Gate Array

network, every member of the network can receive and decrypt all data. TRANSEC is designed to prevent traffic analysis by outside parties.

The FIPS 140-2 evaluated modules are Printed Circuit Boards (PCBs) embedded within a hard, metal case. The Secure Satellite Broadband Solutions are validated at the FIPS 140-2 section levels indicated in Table 1.

Table 1 – Security Level per FIPS 140-2 Section

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

2.2 Module Specification

The physical cryptographic boundary of the Secure Satellite Broadband Solutions is the VT iDirect PCBs that run the iDX firmware (referred to as "FALCON") and its physical interfaces. Per FIPS 140-2 terminology, the Secure Satellite Broadband Solutions are multi-chip embedded modules that meet overall level 2 security requirements. All modules use heat sinks and conformal coating on the boards and tamper evident paint over the screws in order to meet level 2 physical security requirements.

Figure 2 depicts the physical block diagram and the cryptographic boundary of each of the cryptographic modules. The cryptographic boundary is indicated below using the red, dotted line. The diagram also shows the logical interfaces of the modules.

[6] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility

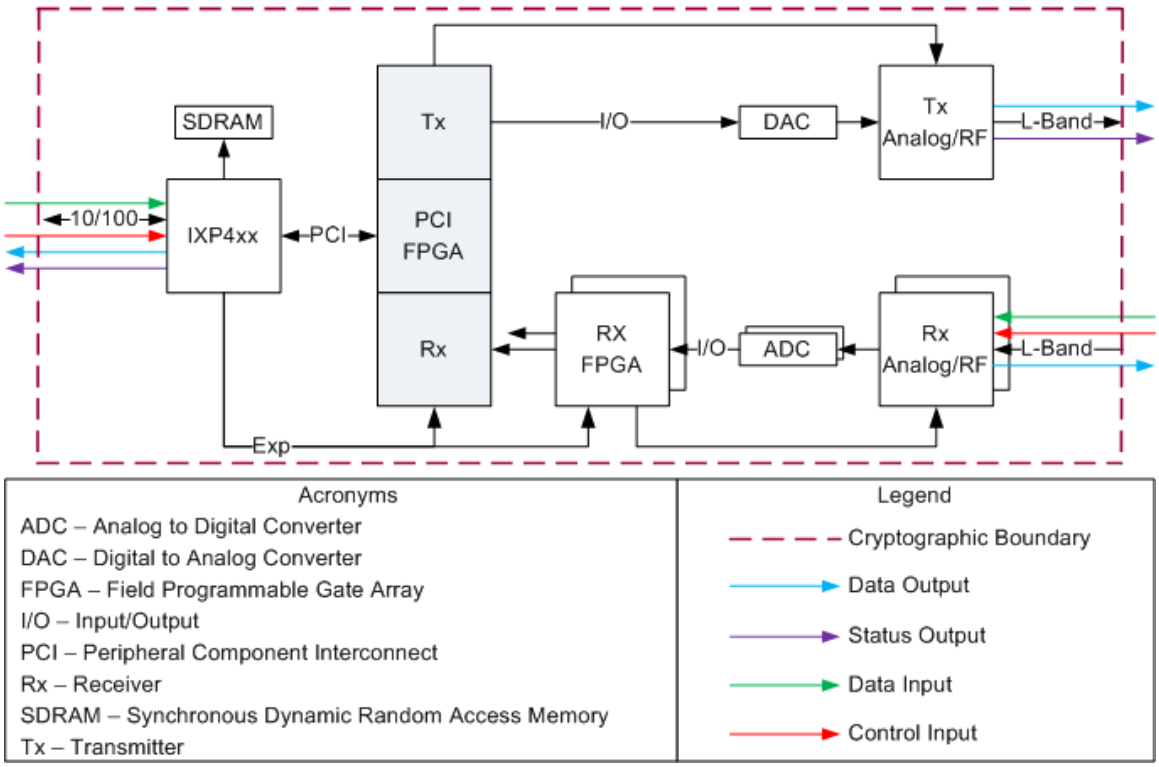

Figure 2 – Cryptographic Module Block Diagram

The VT iDirect Secure Satellite Broadband Solutions router, router board, and line card cryptographic modules share a common design and functionality. Each module uses the same processor and FPGA configuration (shown in Figure 2) to provide secure encryption and decryption of satellite data, voice, and video communications. Each module's cryptographic services and functions are provided by the FALCON firmware release (this validation include versions iDX 3.3.2.5 and iDX 3.4.3.5). Slight, non-security relevant differences in the module hardware implementation are identified by different part numbers. Differences include different form factors, heat dissipation, and quantities of LAN[7] ports and LEDs[8].

2.3 Module Interfaces

The Secure Satellite Broadband Solutions are multi-chip embedded cryptographic modules that meet overall Level 2 FIPS 140-2 requirements.

The physical port mappings for the e800-FIPLSL2 and e8350-FIPSL2 modules are listed in Table 2.

Table 2 – Mapping of the e800-FIPSL2 and e8350-FIPSL2 Physical Ports

Physical Port	Description	Enabled in FIPS Mode of Operation?
Power Connector	MOLEX P/N 501844-1410	Yes
Transmitter (TX Out)	Female coaxial connector	Yes
Receiver (RX Out)	Female coaxial connector	Yes

[7] LAN – Local Area Network
[8] LED – Light Emitting Diode

Physical Port	Description	Enabled in FIPS Mode of Operation?
Receiver (RX In)	Female coaxial connector	Yes
10 MHz[9]	BNC[10] external 10MHz connector (future use)	No
USB[11]	Future Use	No
Console	RJ[12]-45, Serial, RS-232[13]	Yes
LAN A/B	RJ-45, 10/100 Base-T (2 on the e800-FIPSL2, 9 on the e8350-FIPSL2)	Yes
RS-232/GPIO[14]	HD-15, GPIO, Serial	Yes
Power Control	3-pin jumper	Yes

The physical port mapping for the e850MP-FIPLSL2 is listed in Table 3.

Table 3 – Mapping of the e850MP-FIPSL2 Physical Ports

Physical Port	Description	Enabled in FIPS Mode of Operation?
Power Connector	4 pin interface; MOLEX 43650-0400	Yes
Power Control Connector	2 pin interface; MOLEX 43650-0200	Yes
Transmitter, Receivers, GPS	Coaxial Connection	Yes
RS-232/GPIO	20-pin interface: HARWIN M80-8662022	No
LED Connector	20 pin interface; MOLEX 55456-2059	Yes
Ethernet	RJ-45	Yes

The physical port mappings for the EM1D1-FIPLSL2 and M0DM-FIPSL2 modules are listed in Table 4.

Table 4 – Mapping of the EM1D1-FIPSL2 and M0DM-FIPSL2 Physical Ports

Physical Port	Description	Enabled in FIPS Mode of Operation?
Transmitter (TX Out)	Female coaxial connector	Yes
Receiver (RX Out)	Female coaxial connector	Yes
Receiver (RX In)	Female coaxial connector	Yes
LAN A/B, 10/100	LAN RJ-45, 10/100 Base-T	Yes
Console	LAN RJ-45, Configuration Port	Yes
(4) LEDs	Status Indication	Yes

[9] MHz – Megahertz
[10] BNC – Bayonet Neill-Concelman connector
[11] USB – Universal Serial Bus
[12] RJ – Registered Jack
[13] RS-232 – Recommended Standard 232
[14] GPIO – General Purpose Input/Output

Physical Port	Description	Enabled in FIPS Mode of Operation?
Power Connector	PCI[15] interface	Yes

All of the physical interfaces can be categorized into logical interfaces defined by FIPS 140-2, as described in Table 5:

Table 5 – FIPS 140-2 Logical Interfaces

FIPS 140-2 Logical Interface	Secure Satellite Broadband Solutions Port/Interface	Enabled in FIPS Mode of Operation
Data Input	RX In; Ethernet ports; Console port; RS-232/GPIO	Yes
Data Output	TX Out; RX Out; Ethernet ports; Console port; RS-232/GPIO	Yes
Control Input	RX In; Ethernet ports; Console port; RS-232/GPIO	Yes
Status Output	TX Out; Ethernet ports; Console port; RS-232/GPIO	Yes
Power	Power connector	Yes

2.4 Roles, Services, and Authentication

There are two roles in the modules that operators may assume: a Crypto-Officer (CO) role and a User role. The Crypto-Officer is responsible for installing, configuring, and monitoring the modules. The Crypto-Officer accesses the modules remotely over a secured session provided via TLS, SSH, or the satellite channel. The User role is capable of performing diagnostic services in order to determine status of the modules. Users may access the module via the satellite channel.

The modules support multiple concurrent operators. No restrictions are set on the number of operators that may access the modules at once. Module access is determined by which operator is attempting to access the modules.

The modules implement explicit role-based authentication. The CO and User each have a unique username and password assigned to them. An operator assumes the role of CO or User based on which credential they use to login to the modules. Additional information on Authentication is provided in Section 2.4.5.

2.4.1 Crypto-Officer Role

The Crypto-Officer role is responsible for performing installation, configuration, and monitoring services for the modules. The Crypto-Officer can access the modules remotely over a secured session using one of the following methods:

- Remote Command Line Interface (CLI) – The modules can be configured and monitored over a remote CLI management interface using Secure Shell (SSH) version 1.3, 1.5 and 2.0. The Crypto-Officer uses a password to access any services. The modules perform a Diffie-Hellman (DH) key agreement to protect the SSH session. When the Crypto-Officer accesses the module via SSH, he is able to log into the CLI interface directly with the "admin" account and the appropriate password.
- Management Interface over Transport Layer Security (TLS) – The modules can also be configured and monitored using a Graphical User Interface (GUI) over a TLS session, such as the iBuilder and

[15] PCI – Peripheral Component Interconnect

iMonitor applications, which require a user name and password for access. The modules perform RSA authentication and key transport during the TLS handshake.

2.4.2 User Role

The User role is capable of performing diagnostic services in order to determine status of the modules. A User may access the module remotely over a secured session provided via TLS or SSH. Descriptions of these access methods are provided in Section 2.4.1.

2.4.3 CO and User Services

Table 6 lists all CLI services available to a Crypto-Officer and User. Descriptions of the services available are provided in the table below. The following table also list all Critical Security Parameters (CSPs) involved in the services and associated access controls.

Table 6 – Mapping of General Services to Roles, CSPs, and Type of Access

Service	Description	Operator		Type of Access
		CO	User	
authentication	Obtain access to the module	✓	✓	User Password – Read/Execute Crypto-Officer Password – Read/Execute
cert_mgr (line card)	Certificate Manager command	✓		X.509 Certificate – Read/Write Secured Session Key – Read
csp	Enable/disable csp mode	✓		Secured Session Key – Read
fips off	Disable FIPS and enter the non-Approved mode	✓		Secured Session Key – Read
establish SSH session	Establish SSH session using DH public/private key pairing	✓	✓	Secured Session Key – Read/Execute Diffie-Hellman Public Key – Read/Execute Diffie-Hellman Private Key – Read/Execute SSH Authentication Key – Read/Execute HMAC Key – Read/Execute Link Encryption Key –Read/Execute
establish TLS session	Establish TLS session using DH public/private key pairing	✓	✓	Secured Session Key – Read/Execute Diffie-Hellman Public Key – Read/Execute Diffie-Hellman Private Key – Read/Execute Link Encryption Key –Read/Execute
firmware upgrade	Perform firmware upgrade	✓		iDirect Signed Key
key_mgr (line card)	Key manager	✓		Acquisition Ciphertext Channel Key – Read/Write
keyroll_mgr	Keyroll manager command	✓		Dynamic Ciphertext Channel Key – Read/Write Acquisition Ciphertext Channel Key – Read/Write Secured Session Key – Read

Service	Description	Operator		Type of Access
		CO	User	
random	Test random number generator	✓	✓	Secured Session Key – Read/Execute DRBG Seed – Read/Execute DRBG Entropy – Read/Execute DRBG 'V' Value – Read/Execute DRBG 'Key' Value – Read/Execute
reset	Reset machine, restart service, perform self-tests	✓	✓	Secured Session Key – Read/Execute
standby	Place module in standby	✓		Secured Session Key – Read/Execute
status	Display FIPS status	✓	✓	Secured Session Key – Read/Execute
x509	Manage X509 Certificates and RSA keys	✓		X.509 Certificate – Read/Write Secured Session Key – Read/Execute RSA Private Key – Read/Write RSA Public Key – Read/Write
zeroize all	Zeroize all CSPs	✓		All CSPs – Delete

2.4.4 Additional Services

The modules provide services to operators that are not required to assume an authorized role. These services do not require the operator to authenticate to the module. The available services do not modify, disclose, or substitute cryptographic keys and CSPs, or otherwise affect the overall security of the module.

Table 7 maps the services available to operators that are not required to assume an authorized role.

Table 7 – Mapping of Additional Services to Inputs, Outputs, CSPs, and Type of Access

Service	Description	Input	Output	Type of Access
Traffic Throughput	Secured traffic throughput at the data-link layer	Data Link layer packet	Data Link layer packet	Dynamic Ciphertext Channel key - Read
Multicast Packet Reset	After individual component of the multicast packet is extracted and written to the modem's flash memory, the modem resets if the "Reset" option was checked.	"Reset" option is checked	Command status	None

2.4.5 Authentication

The modules implement explicit role-based authentication. The CO and User each have a unique username and password assigned to them. When logging in via SSH or TLS, the CO will login with the 'admin' username. The User will login to the module with the 'user' username. An operator assumes the role of CO or User based on which credential they use to login to the modules. In order for an operator to change roles, they must first log out of the current role they have assumed. This will require the operator to re-authenticate to the modules with the appropriate username and password combination. The results of previous authentications are cleared when the modules are powered off.

A CO and User must authenticate with a username and password. Passwords that are generated by the CO during module initialization shall be a minimum of 8 characters in length and can use any printable US-ASCII[16] character. The probability for guessing an 8-character password that can use 94 different characters for each character in the password is 1 in 94^8, or 1 in 6,095,689,385,410,816.

The fastest network connection supported by the modules is 100 Mbps[17]. Hence at most ($100x10^6$ bits/second × 60 seconds ≈ $6x10^9$ =) 6,000,000,000 bits of data can be transmitted in one minute. Each password is 64 bits (8 bits per character x 8 characters); meaning $9.375x10^7$ passwords can be passed to the module (assuming no overhead) in a one-minute period. This equates to a 1 in 65,020,686 chance of passing in the correct password in a one-minute period.

2.5 Physical Security

The cryptographic modules are multi-chip embedded cryptographic modules per FIPS 140-2 terminology. The modules are PCBs that consist of production grade components and meet Level 2 physical security requirements using heat sinks and conformal coating on the boards and tamper evident paint over the screws.

Figure 3, Figure 4, and Figure 5 below show the iConnex e800-FIPSL2 Satellite Router Board with conformal coating and tamper evident screws. Please note that the e800-FIPSL2 and e8350-FIPSL2 boards have a similar appearance; the only difference is that the e8350-FIPSL2 has a mounted 8-port Ethernet switch.

Figure 3 – iConnex e800-FIPSL2 Satellite Router Board (Bottom)

[16] US-ASCII – United States American Standard Code for Information Interchange
[17] Mbps – Megabits per second

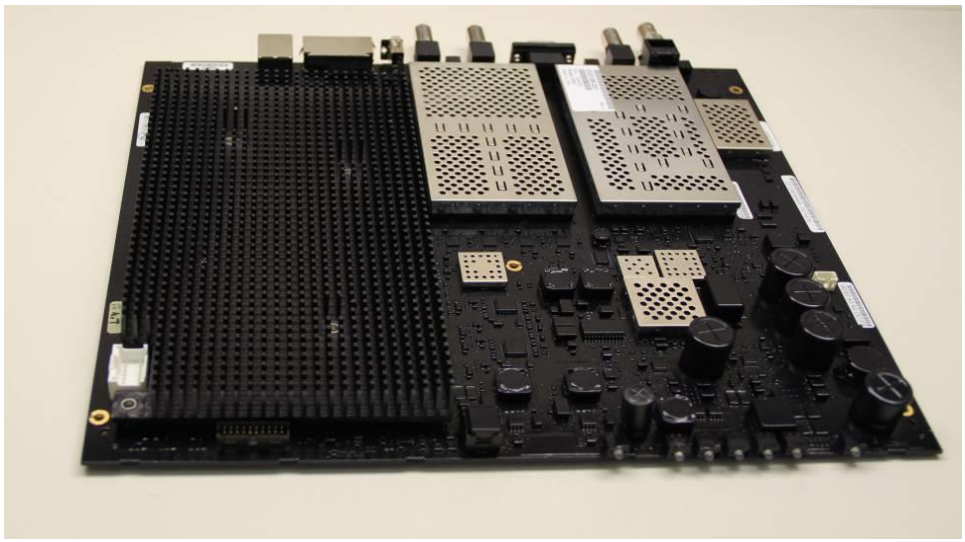

Figure 4 – iConnex e800-FIPSL2 Satellite Router Board (Top)

Figure 5 – iConnex e800-FIPSL2 Satellite Router Board (Top)

Figure 6 and Figure 7 below show the iConnex e8350-FIPSL2 Satellite Router Board with conformal coating and tamper evident screws

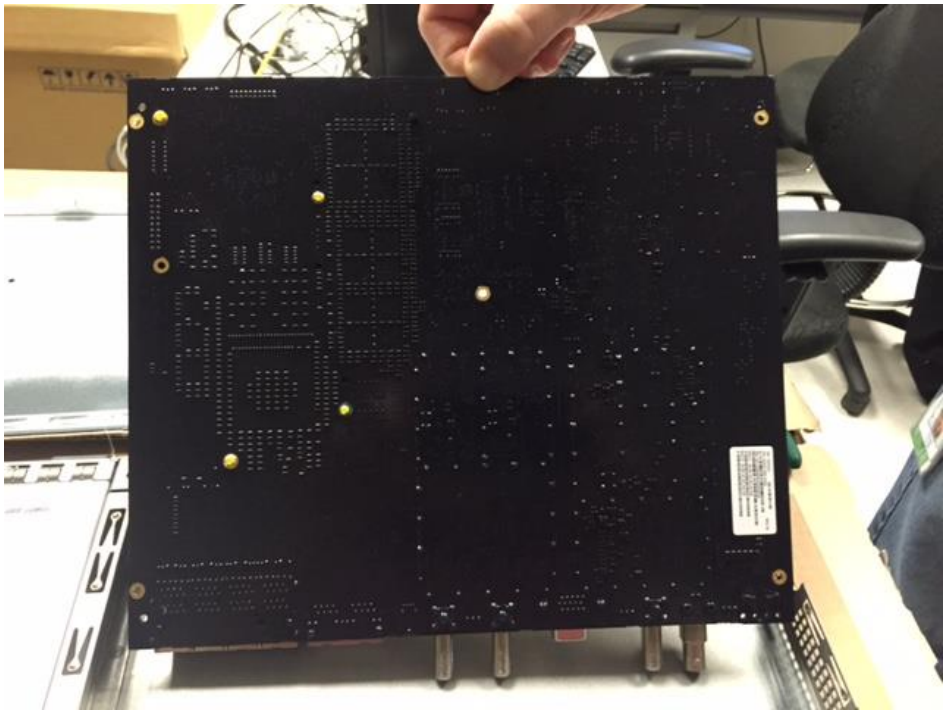

Figure 6 – iConnex e8350-FIPSL2 Satellite Router Board (Bottom)

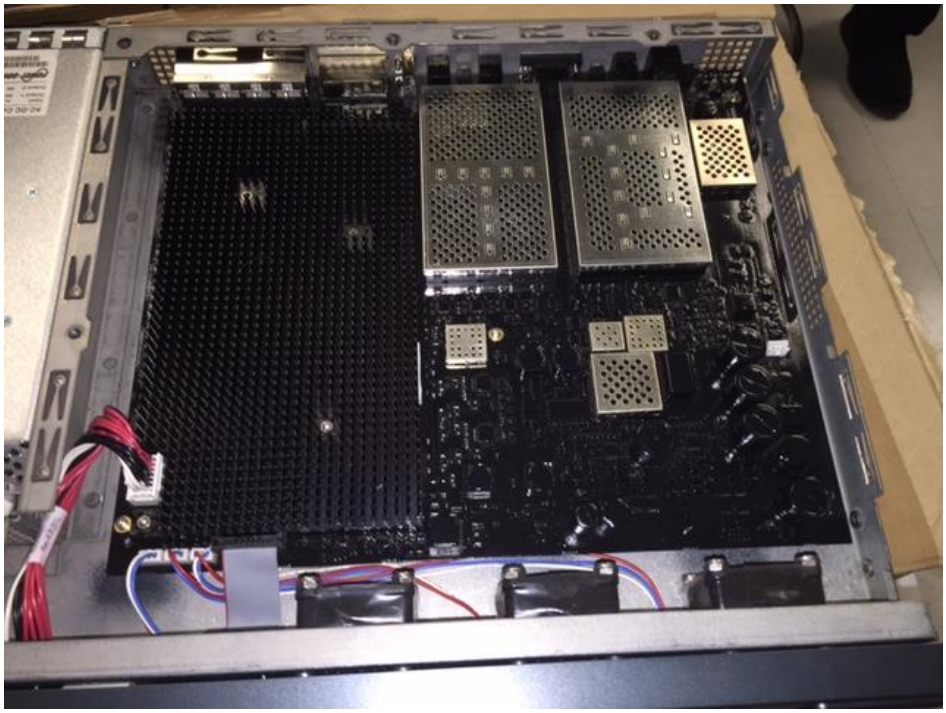

Figure 7 – iConnex e8350-FIPSL2 Satellite Router Board (Top)

Figure 8, Figure 9, and Figure 10 below show the iConnex e850MP-FIPSL2 Satellite Router Board with conformal coating.

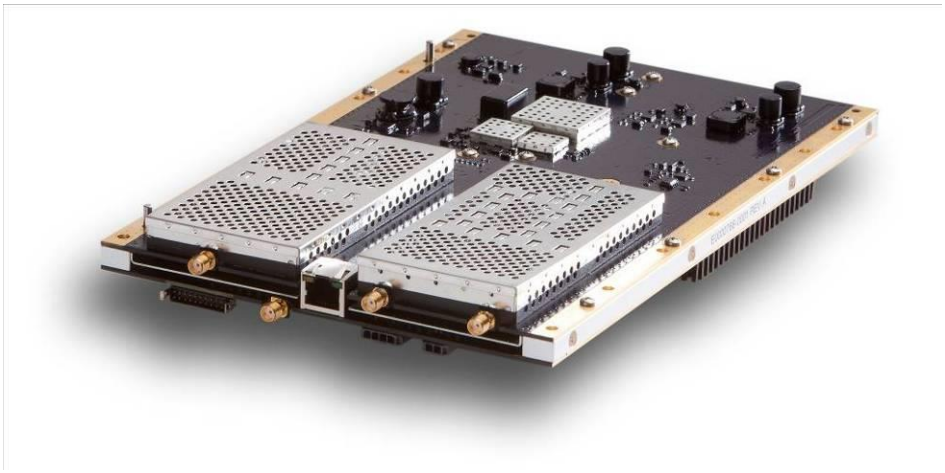

Figure 8 – iConnex e850MP-FIPSL2 Satellite Router Board (Bottom)

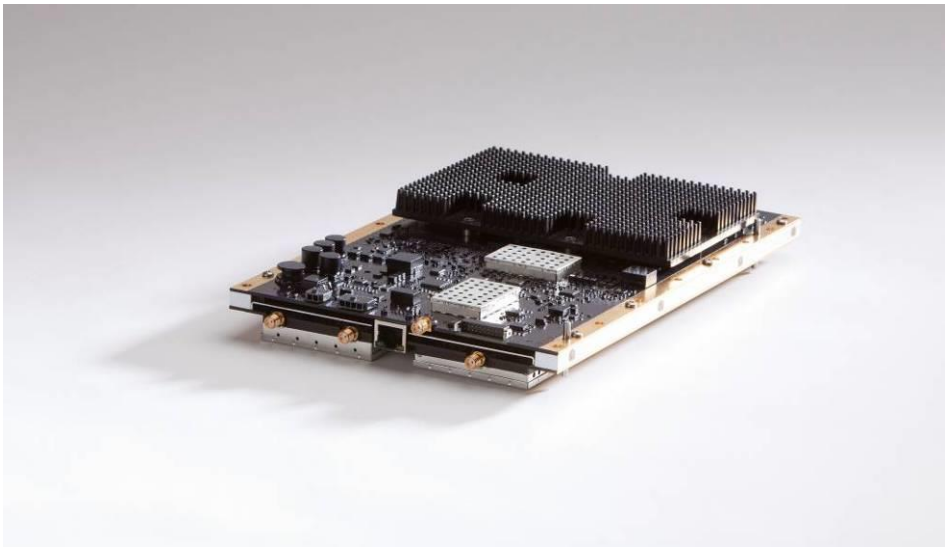

Figure 9 – iConnex e850MP-FIPSL2 Satellite Router Board (Top)

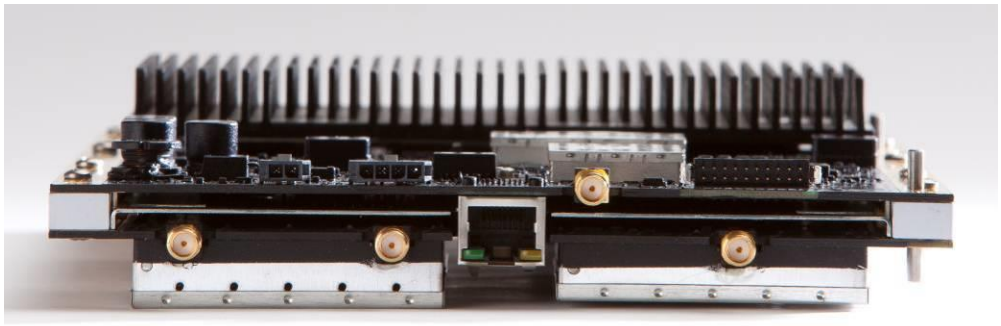

Figure 10 – iConnex e850MP-FIPSL2 Satellite Router Board (Top)

Figure 11, Figure 12, Figure 13, and Figure 14 below show the Evolution eM1D1-FIPSL2 Line Card with conformal coating. Please note that Evolution eM1D1-FIPSL2 and Evolution eM0DM-FIPSL2 Line Cards have the same appearance.

Figure 11 – Evolution eM1D1-FIPSL2 Line Card

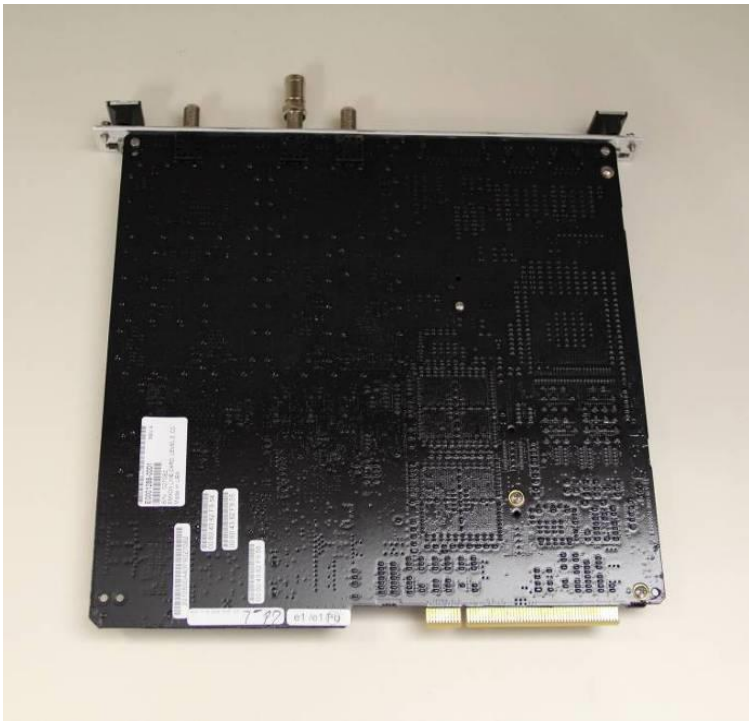

Figure 12 – Evolution eM1D1-FIPSL2 Line Card (Bottom)

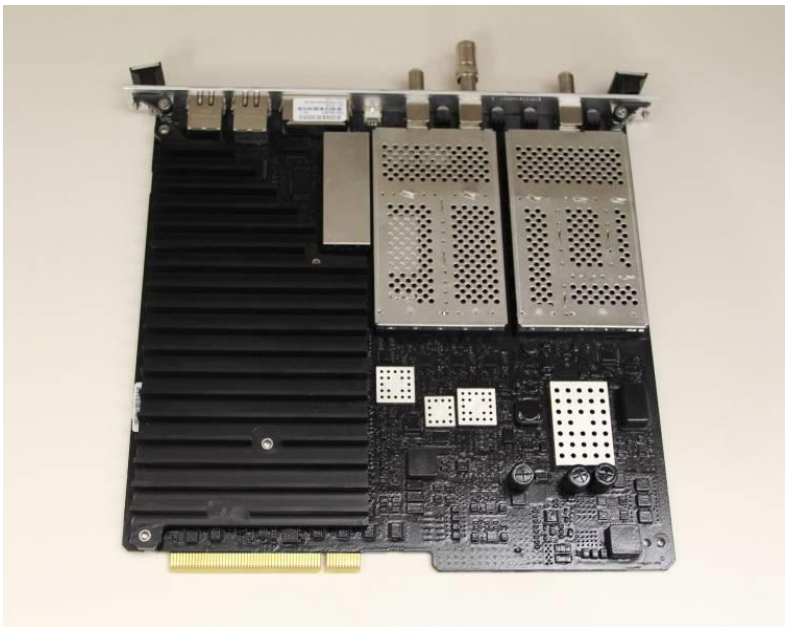

Figure 13 – Evolution eM1D1-FIPSL2 Line Card (Top)

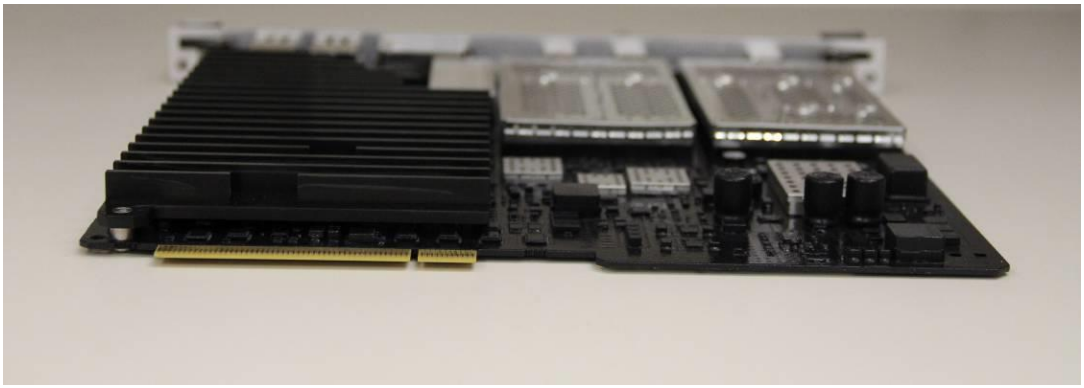

Figure 14 – Evolution eM1D1-FIPSL2 Line Card (Top)

2.6 Operational Environment

The modules' firmware (iDX 3.3.2.5 and iDX 3.4.3.5) runs on Linux OS version 2.6.17.8-uc0-iDirect0 for all the platforms. The operating system protects memory and process space from unauthorized access. The firmware integrity test protects against unauthorized modification of the modules.

2.7 Cryptographic Key Management

The cryptographic modules implement the FIPS-Approved algorithms listed in Table 8.

Table 8 – FIPS-Approved Algorithm Implementations

Algorithm	Certificate Number
AES[18] in CBC[19], CTR[20], and CFB[21] modes – encrypt/decrypt 256-bit key (Firmware Implementation)	3548
AES in CBC mode – encrypt/decrypt 256-bit key (Hardware Implementation)	3603, 3549, 3623
SHA[22]-256, SHA-512	2927
HMAC[23] SHA-256	2267
RSA[24] FIPS 186-4 Key Generation: 2048-bit keys	1828
RSA PKCS[25] #1 v1.5 Signature Generation: 2048-bit keys	1828
RSA PKCS #1 v1.5 Signature Verification: 1024-bit to 2048-bit keys	1828
SP[26] 800-90A CTR_DRBG[27]	904
TLS KDF[28,29]	606
SSH KDF[30]	606

Additionally, the modules utilize the following non-FIPS-Approved but Allowed algorithm implementation:

- Diffie-Hellman 2048 bits key (Key agreement/key establishment methodology provides 112 bits of encryption strength)
- Non-FIPS-Approved PRNG for seeding the SP 800-90A CTR_DRBG
- RSA 2048-bit key encrypt/decrypt (Key wrapping; key establishment methodology provides 112 bits of encryption strength)

[18] AES – Advanced Encryption Standard
[19] CBC – Cipher-Block Chaining
[20] CTR – Counter
[21] CFB – Cipher Feedback Mode
[22] SHA – Secure Hash Algorithm
[23] HMAC – (keyed-) Hash-based Message Authentication Code
[24] RSA – Rivest, Shamir, and Adleman
[25] PKCS – Public Key Cryptography Standard
[26] SP – Special Publication
[27] CTR _DRBG – Counter-based Deterministic Random Bit Generator
[28] KDF – Key Derivation Function
[29] The TLS KDF has not been tested or reviewed by CAVP or CMVP.
[30] The SSH KDF has not been tested or reviewed by CAVP or CMVP.

The modules support the following critical security parameters a described in Table 9.

Table 9 – Cryptographic Keys, Cryptographic Key Components, and CSPs

Key /Component/CSP	Key Type	Generation / Input	Output	Storage	Zeroization	Use
iDirect Signed Key	RSA 2048-bit public key	Externally generated using DRBG	Never exits the module	Hard-coded in the module	Never zeroized	Performs firmware integrity check during power-up and upgrade
Dynamic Ciphertext Channel (DCC) Key	AES-256 CBC key	Externally generated, entered in encrypted form	Never exits the module	Resides in volatile memory in plaintext	By global zeroize command	Provides confidentiality to data over Satellite channel
Secured Session Key	AES-256 CBC key	Generated internally using Diffie-Hellman	Never	Resides in volatile memory in plaintext	Zeroized after session is over	Provides secured channel for management
Acquisition Ciphertext Channel (ACC) Key	AES-256 CBC key	Externally generated by the Protocol Processor, and entered into the remote modem in encrypted form	Never exits the module	Resides in volatile memory in plaintext; resides in plaintext in non-volatile memory	By global zeroize command	Encrypts all traffic and traffic headers required for a remote to acquire the network
Link Encryption Key	AES-256 CBC and CFB key	Internally generated using DRBG or entered in encrypted form	Exits in encrypted form	Resides in volatile memory in plaintext	Zeroized after session is over	Provides confidentiality to Layer 3 data
RSA Private Key	RSA 2048-bit private key	Internally generated using DRBG	Never exits the module	In flash in plaintext	By global zeroize command	Authenticates TLS channel and transports ACC Keys and Link Encryption Key

Key /Component/CSP	Key Type	Generation / Input	Output	Storage	Zeroization	Use
RSA Public Key	RSA 2048-bit public key	Internally generated using DRBG	Exits in plaintext	In flash in plaintext	By global zeroize command	Authenticates TLS channel and transports ACC Keys & Link Encryption Key
Certificates issued by the iDirect Certificate Authority (CA) Foundry	X.509 digital certificates	Externally generated, entered in encrypted form	Exits in encrypted form	In flash in plaintext	By global zeroize command	Used for hub and remote unit validation
Diffie-Hellman private key	224-bit DH private exponent	Internally generated using DRBG	Never exits the module	Resides in volatile memory in plaintext	Zeroized after session is over	Establishes Secured Session Key during SSH or TLS sessions
Diffie-Hellman public key	2048-bit DH public exponent	Internally generated using DRBG	Exits electronicall y in plaintext form	Resides in volatile memory in plaintext	Zeroized after session is over	Establishes Secured Session Key during SSH or TLS sessions
SSH Authentication Key	HMAC-SHA256	Generated internally using DRBG	Never exits the module	Stored inside the volatile memory in plaintext, inside the module	By global zeroize command	Used for data authentication during SSH sessions
Crypto-Officer Password	Password	Entered in plaintext	Never exits the module	Hash value of the password is stored in flash	By global zeroize command	Enables Crypto-Officer role
User Password	Password	Entered in plaintext	Never exits the module	Hash value of the password is stored in flash	By global zeroize command	Enables the User role
HMAC Key	HMAC SHA-256	Internally Generated using DRBG	Never exits the module	Resides in volatile memory in plaintext	Zeroized after session is over	Securely exchange information during SSH session

Key /Component/CSP	Key Type	Generation / Input	Output	Storage	Zeroization	Use
DRBG Seed	Random data – 256 bits	Internally Generated	Never	Keys are not persistently stored by the module	Module reset or power-down	Seeding material for SP 800-90A DRBG
DRBG Entropy[31]	Random data – 128 bits	Internally Generated	Never	Plaintext in volatile memory	Module reset or power-down	Entropy material for SP 800-90A DRBG
DRBG 'V' Value	Internal state value	Internally Generated	Never	Plaintext in volatile memory	Module reset or power-down	Used for CTR_DRBG
DRBG 'Key' Value	Internal state value	Internally Generated	Never	Plaintext in volatile memory	Module reset or power-down	Used for CTR_DRBG

The iDirect Signed Key is a 2048-bit RSA public key hard-coded into the modules. This key is externally generated and is used for verifying the integrity of the modules' firmware during power-up and upgrade. The iDirect Signed Key is stored in flash and never zeroized.

DCC keys are AES CBC 256-bit keys that are used to encrypt/decrypt routing traffic flowing across the satellite network. AES cipher operation using DCC keys is performed by the FPGA implementation of the modules. These keys are generated by the Protocol Processor blade, external to the cryptographic boundary and entered into the modules in encrypted form (RSA key transport). The modules do not provide CO or User access to the DCC keys. These AES keys are stored in volatile memory in plaintext and can be zeroized by using the global zeroize command issued from the CLI.

Secured Session keys are also AES CBC 256-bit keys that are used to provide a secure management session over SSH and TLS. The Secured Session Key is generated internally during DH key agreement. The AES key is stored only in volatile memory and is zeroized upon session termination.

ACC keys are AES CBC 256-bit keys used to encrypt all traffic and traffic headers that are required for a remote to acquire the network. AES cipher operation using ACC keys is performed by the FPGA implementation of the module. These keys are generated by the Protocol Processor blade, external to the cryptographic boundary and entered into the module in encrypted form. When a remote has not been in the network for a long period of time (approx. 2 months) or when a new remote joins the network, it cannot transmit and receive data without the ACC key. In such cases, the ACC key has to be entered by the Crypto-Officer through the secure console port. The AES keys are stored in volatile memory and in non-volatile memory in plaintext. The modules do not provide CO or User access to the ACC keys. They can be zeroized by using the global zeroize command issued from the CLI.

When a modem is configured to have link encryption enabled, it will generate a Link Encryption Key upon initialization. A Link Encryption Key is a 256-bit AES key with CBC or CFB mode. A Link Encryption Key is the unique key used to encrypt and decrypt Layer 3 data with an iDirect remote. Each remote uses a different Link Encryption Key. Notice that in the FIPS mode of operation, link encryption without TRANSEC is not allowed.

[31] The module generates 379-bits of entropy for use in key generation.

The RSA public and private key pair is generated internally by the modules and is used for TLS authentication, key transport. The key pair is stored in flash in plaintext and zeroized by the global zeroize command ("zeroize all"). The RSA key pair can be viewed by the Crypto-Officer in plaintext. At least two independent actions are required to view the RSA private key.

The X.509 certificates on the hubs and remotes are issued by iDirect's CA Foundry as per the instructions in the iBuilder User Guide. These certificates are used in a TRANSEC network for remote and hub unit validation. The certificates are stored in flash in plaintext and zeroized by the global zeroize command ("zeroize all").

The modules perform key agreement during SSH sessions using DH (2048-bit exponent) mechanism. The DH private key is calculated during session initialization and resides only in volatile memory in plaintext. The private key is zeroized after the session is over.

The Crypto-Officer and the User authenticate with passwords. The modules store a SHA-256 based hash value for each password onto the flash and never exports it. The hash value can be zeroized by using the modules' zeroization command.

The DRBG Seed and Entropy are generated from the internal FIPS non-Approved PRNG. These values are stored in volatile memory and can be destroyed by powering down the modules.

The DRBG 'V' and 'Key' values are internal state values unique to the DRBG. These values regulate the operation of the CTR_DRBG. These values are generated by the DRBG instance and are not shared with any other component of the module. Zeroization of these CSPs is achieved by powering down or resetting the module.

2.8 Self-Tests

If any of the power-up or conditional self-tests fail, the modules write an indicator message in the Event log and transition to an error state in which all interfaces are disabled. At this point, data input and data output are inhibited.

An exception to the above paragraph is if the module fails a firmware upgrade test. The firmware upgrade test causes the module to enter a transient error state, which outputs an error indicator and then transitions the module to a normal operational state of the current firmware module. The module will not perform the firmware upgrade and load the upgraded firmware if the firmware upgrade test fails.

The Crypto-Officer may execute on demand self-tests by resetting the module or cycling the modules' power.

2.8.1 Power-Up Self-Tests

The Secure Satellite Broadband Solutions perform the following self-tests at power-up:

- Firmware integrity check using an RSA 2048-bit digital signature with SHA-512
- Known Answer Tests (KATs)
  - AES CBC 256-bit key KAT for encrypt/decrypt (FPGA)
  - AES CFB 256-bit key KAT for encrypt/decrypt (Firmware)
  - SHA-256 and SHA-512 KAT
  - HMAC SHA-256 KAT

- Triple-DES CBC KAT for encrypt/decrypt [32]
- RSA KAT for sign/verify
- SP 800-90A CTR_DRBG KAT

2.8.2 Conditional Self-Tests

The Secure Satellite Broadband Solutions perform the following conditional self-tests:

- Continuous random number generator test for the DRBG
- Continuous random number generator test for the entropy gathering
- RSA pair wise consistency check
- Firmware upgrade test

2.8.3 Critical Function Tests

The Secure Satellite Broadband Solutions perform the following critical function tests:

- DRBG Instantiate
- DRBG Generate
- DRBG Reseed
- DRBG Uninstantiate

2.9 Mitigation of Other Attacks

This section is not applicable. The modules do not claim to mitigate any attacks beyond the FIPS 140-2 Level 2 requirements for this validation.

[32] The Triple-DES algorithm is not available for use even though the KAT is performed. Failure of this KAT will result in an error.

3 Secure Operation

The Secure Satellite Broadband Solutions meet overall Level 2 requirements for FIPS 140-2. The sections below describe how to place and keep the module in FIPS-approved mode of operation.

3.1 Crypto-Officer Guidance

The Crypto-Officer is responsible for installing, configuring, and monitoring the modules. Upon receiving the modules, the Crypto-Officer must properly secure the modules per the instruction provided in Section 2.5. The CO shall periodically check the modules for tamper evidence by looking for scratches and cracks in the conformal coating. Should the CO suspect that a module has been tampered with, they should contact VT iDirect support teams:

- For iDirect Government Technologies (iGT) customers, at +1 703 648 8111 or http://tac.idirectgt.com.
- For VT iDirect Customers, +1 703 648 8151 or http://tac.idirect.net.

The Crypto-Officer can access the modules remotely over a secured session. Remote secured sessions are provided via TLS and SSH.

3.1.1 Initialization

The modules must be configured for use in a TRANSEC-enabled network using a TRANSEC-enabled Protocol Processor and the iBuilder application. All network elements that are subsequently created under a TRANSEC-enabled protocol processor will become part of the TRANSEC-compliant network. This process involves configuring the option file for each respective module via the external iBuilder desktop application. To configure each module the CO shall:

1. Enter the device type, serial number, and Satellite and LAN[33] IP addresses in iBuilder
    a. Ensure the modem is part of a TRANSEC network
2. Un-check the "Disable Authentication" option
3. Generate certificates via the CA Foundry provided by VT iDirect's Network Management System (NMS)
4. Generate a secure password for both the "Admin" (CO) and "User" accounts, making sure that a minimum of 8 characters is used in each password.
5. Generate a new "options file"
6. Load the "Options File" onto the module.
7. Use the FIPS-Approved RSA key transport method to retrieve an existing ACC key that is part of the TRANSEC network with an operator defined pass phrase. Input the ACC key and pass phrase into the module.
8. Reboot the module.

The module is now configured for the FIPS-Approved mode. Note that, while operating in the FIPS-Approved mode of operation, no bypass services are supported. In-depth and detailed guidance for configuring, operating, and maintaining an iDirect satellite network is in the *iDirect Network Management System iBuilder's User Guide v3.3*.

3.1.2 Management

The Crypto-Officer shall monitor the modules' status by regularly checking the Statistics log. If the Crypto-Officer notices any irregular activity or module errors, then they should contact VT iDirect Technologies customer support. The CO or User can determine the current mode of operation by entering the "status" command into the FALCON CLI

[33] LAN – Local Area Network

3.2 User Guidance

The User role is able to access the modules over the satellite network and execute commands that are not security-relevant. See Table 6 above for a list of commands available to the User role.

3.3 Non-Approved Mode

VT iDirect ships the Secure Satellite Broadband Solutions in the non-Approved mode. Instructions to bring the modules into the Approved mode are provided in Section 3.1.1. It is also possible to enter the non-Approved mode from the Approved mode using the FALCON CLI. While operating in the non-Approved mode, the modules provide access to additional services and physical ports. To transition the Secure Satellite Broadband Solutions to the non-Approved mode from the Approved mode:

1. Execute the "csp enable" command
2. Zeroize the CSPs with the "zeroize all" command
3. Execute the "fips off" command
4. Reboot the module

Following reboot, the modules will be operating in the non-Approved mode. An operator can determine the current mode of operation by entering the "status" command into the FALCON CLI.

3.3.1 Services Available in Non-Approved Mode

The module provides services to operators in addition to those listed Section 2.4.3. Additional non-Approved services include:

- Access Operating System CLI
- Plaintext key input
- Access root shell of the modules via telnet or SSH
- Access root shell of the module via RS-232 connection
- Non-compliant Password Based Key Derivation Function

When accessing the services listed in Section 2.4.3 while operating in the non-Approved mode, the services shall be considered "non-compliant" as they do not provide the same security as when executed in the Approved mode of operation. The services listed in Section 2.4.4 are not available to operators when operating in the non-Approved mode.

3.3.2 Security Functions Available in Non-Approved Mode

While operating in the non-Approved mode, the modules provide access to the Security Functions below:

- AES in CBC and CFB modes – encrypt/decrypt 256-bit key (Firmware Implementation)
- SHA-256, SHA-512
- HMAC SHA-256
- RSA Key Generation – 2048-bit key
- RSA sign/verify – 1024-bit to 2048-bit keys
- SP 800-90A CTR_DRBG
- TLS Key Derivation Function
- SSH Key Derivation Function
- Password Based Key Derivation Function

4 Acronyms

Table 10 provides a list of acronyms used throughout this document.

Table 10 – Acronyms

Acronym	Definition
ACC	Acquisition Ciphertext Channel
AES	Advanced Encryption Standard
ASCII	American Standard Code for Information Interchange
BNC	Bayonet Neill-Concelman connector
BUC	Block Upconverter
CA	Certificate Authority
CBC	Cipher Block Chaining
CFB	Cipher Feedback Mode
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
CSP	Critical Security Parameter
CTR_DRBG	Counter-based Deterministic Random Bit Generator
DAC	Digital to Analog Converter
DH	Diffie-Hellman
DVB-S2	Digital Video Broadcast – Satellite – Second Generation
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
FPGA	Field Programmable Gate Array
GPIO	General Purpose Input/Output
GPS	Global Positioning System
HDLC	High-Level Data Link Control
HMAC	(keyed-) Hash-based Message Authentication Code
IP	Internet Protocol
KAT	Known Answer Test
KDF	Key Derivation Function
LAN	Local Area Network
LED	Light Emitting Diode
LNB	Low-noise Block Downconverter

Acronym	Definition
Mbps	Megabits per second
MHz	Mega Hertz
NIST	National Institute of Standards and Technology
NMS	Network Management Server
OS	Operating System
PCB	Printed Circuit Board
PCI	Peripheral Component Interconnect
PKCS	Public Key Cryptography Standard
PRNG	Pseudo Random Number Generator
RF	Radio Frequency
RJ	Registered Jack
RS-232	Recommended Standard 232
RSA	Rivest Shamir and Adleman
RX	Receiver Coaxial Connector
SHA	Secure Hash Algorithm
SP	Security Policy
SSH	Secure Shell
TDMA	Time Division Multiple Access
TLS	Transport Layer Security
TRANSEC	Transmission Security
TX	Transmitter Coaxial Connector
ULC	Universal Line Card

Prepared by:
Corsec Security, Inc.

13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America
Phone: +1 (703) 267-6050
Email: info@corsec.com
http://www.corsec.com