VT iDirect, Inc.

Secure Satellite Broadband Solutions

Modules Names: Evolution e8350 – Satellite Router [1], iConnex e800 –Satellite Router Board [2], iConnex e850MP – Satellite Router Board [3], iConnex e850MP-IND Satellite Router Board [4], iConnex e850MP-IND with Heat Sink Satellite Router Board [5], Evolution eM1D1 – Line Card [6], and Evolution eM0DM – Line Card [7]
Firmware Version: iDX version 2.3.1
Hardware Versions: E0000051-0003 [1], E0001340-0002 [2], E0000731-0001 [3], E0000731-0002 [4], E0000731-0003 [5], E0000080-0002 [6], and E0000080-0005 [7]

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 1
Document Version: 1.2

Prepared for:

VT iDirect, Inc.
13921 Park Center Road, Suite 600
Herndon, VA 20171
United States of America

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

Prepared by:

Corsec Security, Inc.
13135 Lee Jackson Memorial Highway, Suite 220
Fairfax, VA 22033
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™ - Satellite Router (Part #E0000051-0003)
- iConnex e800™ - Satellite Router Board (Part # E0001340-0002)
- iConnex e850MP™ - Satellite Router Board (Part # E0000731-0001, E0000731-0002, E0000731 - 0003)
- Evolution eM1D1™ - Line Card (Part #E0000080-0002)
- Evolution eM0DM™ - Line Card (Part #E0000080-0005)

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 Canada (CSEC) 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 1 FIPS 140-2 validation of the modules. The Evolution e8350 Satellite Router, iConnex e800 Satellite Router Board, iConnex e850MP Satellite Router Board, iConnex e850MP-IND Satellite Router Board, iConnex e850MP-IND with Heat Sink Satellite Router Board, Evolution eM1D1 Line Card, and Evolution eM0DM 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 one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Model document
- Other supporting documentation as additional references

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to VT iDirect. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Submission Package is proprietary to VT iDirect and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact VT iDirect.

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 deterministic Time Division Multiple Access (TDMA) upstream carrier and DVB-S2[2] downstream carrier. The VT iDirect TDMA network is optimized for satellite transmissions, squeezing the maximum performance out of the bandwidth provided by satellite links. 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, Protocol Processor, Hub Line Card, and the Ethernet switch with remote modem. In a star topology, the protocol processor acts as the central network controller, the Hubl Line Card is responsible for the hub side modulation and demodulation (modem) functions, and the remote modem provides modem functionalities for the Ethernet switch. A common deployment of the VT iDirect network components is shown below.

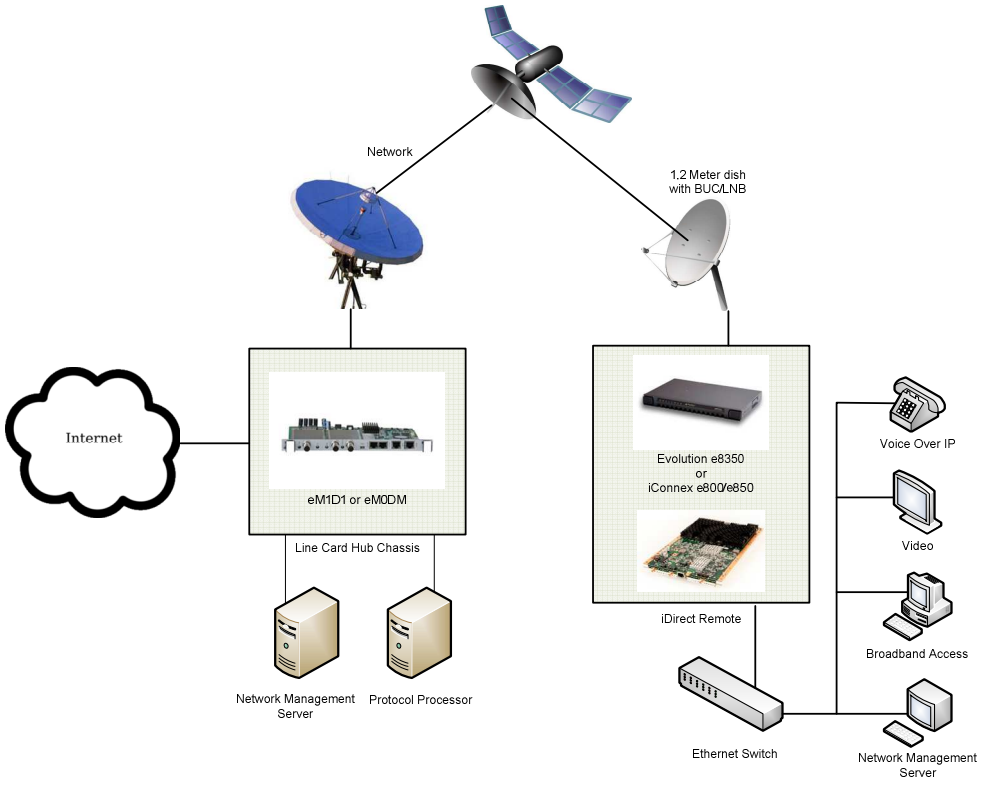

Figure 1 – iDirect Network Deployment

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

VT iDirect's hardware modules offer the Transmission Security (TRANSEC) feature that enables encryption to all Data Link Layer traffic including all control and management data flowing between the ULC and Remote modem using the Advanced Encryption Standard (AES). VT iDirect achieves full TRANSEC compliance by presenting to an adversary eavesdropping on the RF[3] link a constant wall of fixed-sized, strongly-encrypted traffic segments, the frequency 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 indeterminate 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 a Star network then share their exclusive key set. Encryption of data occurs in FPGA[4] firmware. TRANSEC encrypts all data in Layer 2, so even the High-level Data Link Control (HDLC) sources and destinations of packets are encrypted. Multicast and broadcast data is also encrypted. Since the key set is shared among the network, every member of the network can receive and decrypt all data. TRANSEC is designed to prevent traffic analysis by outside parties.

Link Encryption occurs completely in the module firmware. Each remote and its counter-part layer in the protocol processor creates a transmit key (Link Encryption Key, See Table 11) and distributes this to its peer, using the same key transport method as TRANSEC. Link Encryption is point-to-point, so each remote has a unique key for receiving and transmitting data. Layer 2 data, such as source and destination link addresses, is not encrypted. When used without TRANSEC, broadcast and multicast traffic is not encrypted. Therefore, link level information, such as HDLC destinations, is not protected by Link Encryption.

The cryptographic modules provide secure traffic routing services. The platforms for the cryptographic modules are Printed Circuit Boards (PCBs) for the following:

- Evolution e8350™ Satellite Router (Part # E0000051-0003)
- iConnex e800™ Satellite Router Board (Part # E0001340-0002)
- iConnex e850MP™ Satellite Router Board (Part # E0000731-0001, E0000731-0002, E0000731-0003)
- Evolution eM1D1™ Line Card (Part # E0000080-0002)
- Evolution eM0DM™ Line Card (Part # E0000080-0005)

The module firmware runs on version 2.6.17.8-uc0-iDirect0of the Linux Operating System (OS) for all the platforms. The Secure Satellite Broadband Solutions are validated at the following FIPS 140-2 Section levels:

Table 1 – Security Level per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1

[3] RF – Radio Frequency
[4] FPGA – Field Programmable Gate Array

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

2.2 Module Specification

The cryptographic boundary of the modules is the VT iDirect PCBs that run the iDX firmware, which is referred to as "FALCON". Per FIPS 140-2 terminology, the Secure Satellite Broadband Solutions are multi-chip embedded modules that meet overall level 1 security requirements. Physically, the PCB is the cryptographic boundary.

Figure 2 depicts the physical block diagram and the cryptographic boundary of the modules, which is indicated below using the red dotted line. The diagram also shows the logical interfaces with the modules. The red arrow indicates control input. The blue arrow indicates data output. The green arrow indicates data input. The purple arrow indicates status output.

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

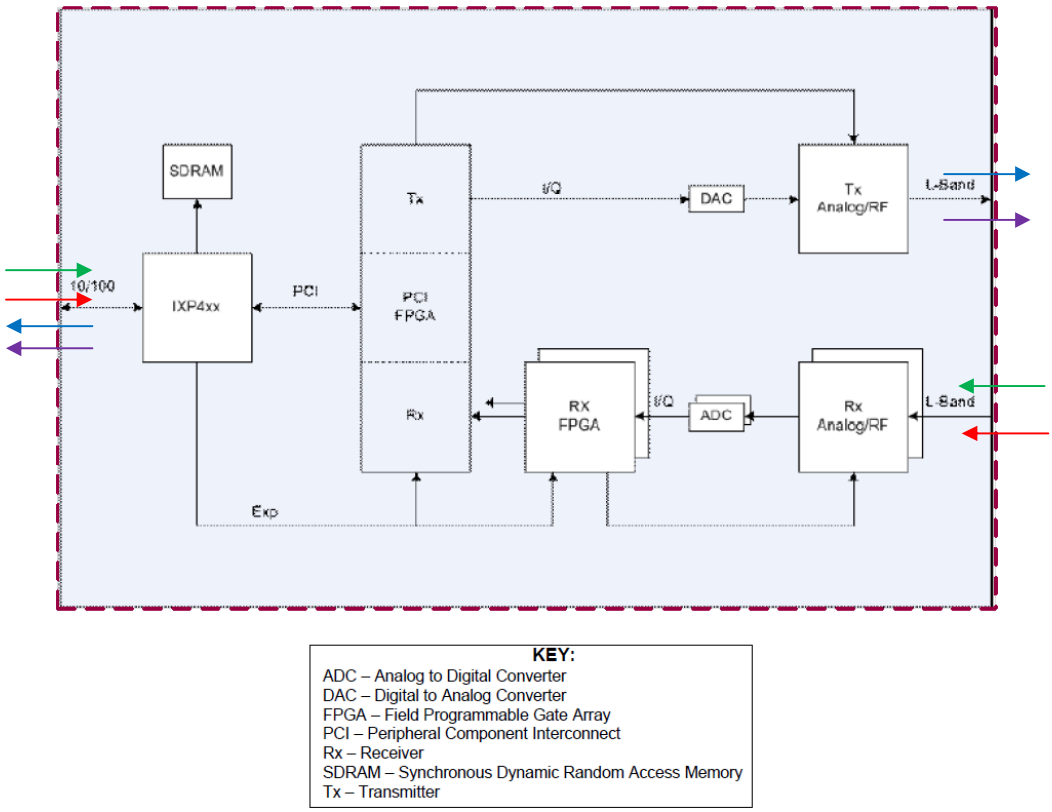

Figure 2 – Cryptographic Module Block Diagram

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. The cryptographic services and functions provided by each module are provided by the same FALCON firmware release (iDX 2.3.1). Slight non-security relevant differences in the module hardware implementation are indentified by different part numbers, including different form factors, heat dissipation, quantities of LAN[6] ports and LEDs[7], and other part differences.

2.3 Module Interfaces

The Secure Satellite Broadband Solutions are multi-chip embedded cryptographic modules that meet overall Level 1 FIPS 140-2 requirements. The physical port mapping for the modules are listed in the tables below:

Table 2 – Mapping of the e800 and e8350 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

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

Physical Port	Description	Enabled in FIPS Mode of Operation.
Receiver (RX Out)	Female coaxial connector	Yes
Receiver (RX In)	Female coaxial connector	Yes
10 MHz[8]	BNC[9] external 10MHz connector (future use)	No
USB[10]	Future Use	No
Console	RJ[11]-45, Serial, RS-232[12]	Yes
LAN A/B	RJ-45, 10/100 Base-T (2 on the e800, 9 on the e8350)	Yes
RS-232/GPIO[13]	HD-15, GPIO, Serial	No
Power Control	3-pin jumper	Yes

Table 3 – Mapping of the e850MP, e850MP-IND, and e850MP-IND with Heat Sink 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

Table 4 – Mapping of the eM1D1 and eM0DM 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

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

Physical Port	Description	Enabled in FIPS Mode of Operation?
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
Power Connector	PCI[14] interface	Yes

The choice of how to display the LEDs on the modules is determined by the integrator of the PCBs. The LED functions are handled by the FALCON application.

All of the interfaces that are enabled, as well as physical interfaces, can be categorized into logical interfaces defined by FIPS 140-2, as described in the following table:

Table 5 – FIPS 140-2 Logical Interfaces

FIPS 140-2 Logical Interface	Secure Satellite Broadband Solutions Port/Interface
Data Input	Rx, Ethernet ports, console port
Data Output	Tx, Ethernet ports, console port
Control Input	Rx, Ethernet ports, console port
Status Output	Tx, Ethernet ports, console port
Power	Power connector

2.4 Roles, Services, and Authentication

There are three roles in the module that operators may assume: Crypto-Officer role, User role, and Client User role. Please note that, as the cryptographic modules were validated against Level 1 requirements, they do not support role-based or identity-based authentication.

2.4.1 Crypto-Officer Role

The Crypto-Officer role is implicitly assumed when performing installation, configuration, or monitoring services for the modules. The Crypto-Officer accesses the modules locally over the console port or remotely over a secured session. There are four different interfaces that can be used for management purposes:

- Console – The Crypto-Officer locally manages the modules by directly connecting through the console port (Serial over RJ45). The Crypto-Officer has to use an account name of “admin” and a password to access any services. The Crypto-Officer is authorized to change its own password and the passwords of User Role accounts (“user” and “diagnostic”).

[14] PCI – Peripheral Component Interconnect

- 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 mechanism to initialize 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 version 1.0 session, such as the iBuilder and iMonitor applications which require a user name and password for access. The modules perform RSA authentication and key transport during the TLS handshake.
- Management over Satellite – Over the satellite channel, the modules can perform low-level configuration and monitoring (all non-security-relevant). This consists of low-level link management (such as timeplans) sent by the protocol processor to the modules for which authentication is not required. The protocol processor will only send Layer 2 Reset messages when prompted to do so by a password privileged user.

2.4.2 User Role

The User has the ability to access the falcon console over the satellite network. On the console, the User is enabled with account name "user" or "diagnostic" and a password to access any services. Accounts "user" and "diagnostic" employ the same password mechanism. Passwords are configured and controlled by the Crypto-Officer with the "admin" account. The "user" and "diagnostic" accounts do not have the privilege to change passwords. The services available to the User role ("user" and "diagnostic" accounts) do not involve viewing or modifying CSPs. See Table 6, Table 7, and Table 8 for a list of User services.

2.4.3 Client User Role

The Client User accesses the modules over the Ethernet ports and utilizes the modules' traffic routing and link encryption services. The Client User role is implicitly assumed by a network device or application routing traffic through the modules.

2.4.4 Services

Table 6, Table 7, and Table 8 list all CLI services available to a Crypto-Officer and User. The CLI services can be categorized in three different groups as follows:

1. General Services: Common functions to the iDX firmware.
2. Hub Specific Services: These services are only accessible on the eM1D1 and eM0DM Line Card platforms.
3. Remote Specific Services: Services specific to the Evolution e8350 Satellite Router, iConnex e800, iConnex e850MP, iConnex e850MP-IND, and iConnex e850MP-IND with Heat Sink Satellite Router Boards.

Descriptions of the services available are provided in the tables below. The following tables 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	
Antenna/debug	AntennaClient st	✓	✓	Secured Session Key – Read
Antenna/params	Stats| params | debug	✓	✓	Secured Session Key – Read

Service	Description	Operator		Type of Access
		CO	User	
Antenna/point	Points to currently defined settings in [SATELLITE] group	✓	✓	Secured Session Key – Read
arp	Address Resolution Protocol (ARP) control	✓	✓	Secured Session Key – Read
beam/debug	Sets debug level for beam switch module	✓	✓	Secured Session Key – Read
beamselector/control	Beam selector control command	✓	✓	Secured Session Key – Read
beamselector/list	List known beams	✓	✓	Secured Session Key – Read
beamselector/lock	Suppress the timer and stay on this beam	✓	✓	Secured Session Key – Read
beamselector/mapsize	Print or change the map size request params	✓	✓	Secured Session Key – Read
beamselector/newmap	Force a request for a new map	✓	✓	Secured Session Key – Read
beamselector/params	Stats | params | debug	✓	✓	Secured Session Key – Read
beamselector/switch	Switch to new beam	✓	✓	Secured Session Key – Read
clear	Clear screen	✓	✓	Secured Session Key – Read
console	Console control	✓	✓	Secured Session Key – Read
date	Get the downstream time information	✓	✓	Secured Session Key – Read
delay	Usage: delay <msecs to sleep>	✓	✓	Secured Session Key – Read
dgm_pkg_rx	Datagram Package Download Receiver control	✓		Secured Session Key – Read
dma	Direct Memory Access (DMA) statistics	✓	✓	Secured Session Key – Read
eloop	Display event loop status	✓	✓	Secured Session Key – Read
ENTER_ERROR_STATE	Enter Error state	✓		Secured Session Key – Read
ENTER_RECOVERY_STATE	Start recovery falcon	✓	✓	Secured Session Key – Read
error_status	Display error status string	✓	✓	Secured Session Key – Read

Service	Description	Operator		Type of Access
		CO	User	
eth	Configure a network interface	✓	✓	Secured Session Key – Read
eth_monitor	Ethernet Interface Monitor	✓		Secured Session Key – Read
extras	Extras option file manipulation	✓	✓	Secured Session Key – Read
fll	Allows to query the status of the hardware's frequency lock loop	✓	✓	Secured Session Key – Read
fpga	FPGA Rx1 driver	✓	✓	Secured Session Key – Read
fpga/rx	FPGA Rx Driver	✓	✓	Secured Session Key – Read
fpga/tx	FPGA Tx Driver	✓	✓	Secured Session Key – Read
gecho	Global echo	✓	✓	Secured Session Key – Read
heap	Memory usage	✓	✓	Secured Session Key – Read
hub_fsd	Hub FSD	✓	✓	Secured Session Key – Read
igmp	Multicast control	✓	✓	Secured Session Key – Read
ip	Router control	✓	✓	Secured Session Key – Read
keyroll_mgr	Keyroll manager command	✓		Dynamic Ciphertext Channel Key – Read/Write Acquisition Ciphertext Channel Key – Read/Write Secured Session Key – Read
laninfo	View IP address/netmask	✓	✓	Secured Session Key – Read
latlong	LAT LONG	✓	✓	Secured Session Key – Read
license	Get license	✓	✓	Secured Session Key – Read
licensestat	Remote license status information	✓	✓	Secured Session Key – Read

Service	Description	Operator		Type of Access
		CO	User	
mac	Media Access Control (MAC) control	✓	✓	Secured Session Key – Read
mapclient/control	Map client control command	✓	✓	Secured Session Key – Read
mapclient/params	Stats | params | debug	✓	✓	Secured Session Key – Read
maphandler/control	Map handler control command	✓	✓	Secured Session Key – Read
maphandler/params	Stats | params | debug	✓	✓	Secured Session Key – Read
mem	Resource information	✓	✓	Secured Session Key – Read
netstat	Checks network configuration and activity	✓	✓	Secured Session Key – Read
nms_echo	NMS event echo	✓	✓	Secured Session Key – Read
nmsr	Debug network management system Reporting object (event message sender)	✓	✓	Secured Session Key – Read
oob	Out of Band (OOB) control	✓	✓	Secured Session Key – Read
options	Options file manipulation	✓	✓	Secured Session Key – Read
packages	Show list of installed software packages and their versions	✓	✓	Secured Session Key – Read
params	View/edit global parameters	✓	✓	Secured Session Key – Read
pasoc	Command for the packet socket layer	✓	✓	Secured Session Key – Read
passwd	Change password	✓		Password – Read, Write Secured Session Key – Read
pcmd	Periodic console Command	✓	✓	Secured Session Key – Read
ping	Utility	✓	✓	Secured Session Key – Read
profiling	Profiling the Utils	✓	✓	Secured Session Key – Read

Service	Description	Operator		Type of Access
		CO	User	
ps	Show the output of the ps command	✓	✓	Secured Session Key – Read
reset	Reset machine or restart service	✓	✓	Secured Session Key – Read
rx/enable	Rx Enable	✓		Secured Session Key – Read
rx/frequency	Rx Frequency	✓	✓	Secured Session Key – Read
rx/ifl10	Rx IFL 10M	✓	✓	Secured Session Key – Read
rx/iflDC	Rx IFL DC	✓	✓	Secured Session Key – Read
rx/ifltone	Rx IFL 22k tone	✓	✓	Secured Session Key – Read
rx/power	Rx Power	✓	✓	Secured Session Key – Read
rx/symrate	Rx Symbol rate	✓		Secured Session Key – Read
rx2/agc	Rx AGC	✓	✓	Secured Session Key – Read
rx2/bitrate	Rx BitRate	✓		Secured Session Key – Read
rx2/cof	Rx Frequency Offset	✓	✓	Secured Session Key – Read
rx2/ enable	Rx enable	✓		Secured Session Key – Read
rx2/frequency	Rx Frequency	✓	✓	Secured Session Key – Read
rx2/symrate	Rx Symbolrate	✓		Secured Session Key – Read
rxdiag/14DCVoltage	14 DC Voltage	✓	✓	Secured Session Key – Read
rxdiag/6DCVoltage	6 DC Voltage	✓	✓	Secured Session Key – Read
rxdiag/7DCVoltage	7 DC Voltage	✓	✓	Secured Session Key – Read
rxdiag/rxpower	Rx RF Composite Power	✓	✓	Secured Session Key – Read
rxdiag/temperature	Board temperature	✓	✓	Secured Session Key – Read

Service	Description	Operator		Type of Access
		CO	User	
rxdiag/tx10M	Tx 10M output	✓	✓	Secured Session Key – Read
rxdiag/txpower	Tx RF Composite Power	✓	✓	Secured Session Key – Read
service	Service start/stop command	✓		Secured Session Key – Read
sn	Show modem serial number	✓	✓	Secured Session Key – Read
Stats	View/Edit global stats	✓	✓	Secured Session Key – Read
status	Show status of stack	✓	✓	Secured Session Key – Read
sys_time	Sys Time Tick	✓	✓	Secured Session Key – Read
systray	Debugs systray messages (mulicast messages sent on the Local Access Network or LAN)	✓	✓	Secured Session Key – Read
tick	Get time tick	✓	✓	Secured Session Key – Read
timer	Timer control	✓	✓	Secured Session Key – Read
tlev	Trace control	✓	✓	Secured Session Key – Read
tls	Transport Layer Security (TLS) control	✓	✓	Secured Session Key – Read
tls_mnc	Debugs the secure MnC control server	✓	✓	Secured Session Key – Read
transec	TRANSEC related Field Programmable Gate Array (FPGA) registers stats	✓		Secured Session Key – Read
tx/alcdac	Tx ALCDAC	✓		Secured Session Key – Read
tx/atten	Tx Atten	✓		Secured Session Key – Read
tx/atten1	Tx Atten1	✓		Secured Session Key – Read
tx/atten2	Tx Atten2	✓		Secured Session Key – Read
tx/cw	Tx CW	✓		Secured Session Key – Read

Service	Description	Operator		Type of Access
		CO	User	
tx/enable	Tx Enable	✓		Secured Session Key – Read
tx/freq	Tx frequency	✓	✓	Secured Session Key – Read
tx/halfdb	Tx Halfdb Atten	✓		Secured Session Key – Read
tx/ifl10	Tx IFL 10M	✓	✓	Secured Session Key – Read
tx/iflDC	Tx IFL DC	✓	✓	Secured Session Key – Read
tx/iqoffset	TX IQ Offset	✓		Secured Session Key – Read
tx/pn	Tx PN	✓		Secured Session Key – Read
tx/power	Tx Power	✓	✓	Secured Session Key – Read
tx/ssb	Tx ssb Pattern	✓	✓	Secured Session Key – Read
tx/symrate	Tx Symbolrate	✓		Secured Session Key – Read
uptime	System and application uptime	✓	✓	Secured Session Key – Read
version	Build information	✓	✓	Secured Session Key – Read
versions_report	Full operating environment report	✓	✓	Secured Session Key – Read
x509	Manage X509 Certificates and RSA keys	✓	✓	RSA Private Key – Read/Write RSA Private Key – Read/Write Secured Session Key – Read
xoff	Disallow messages from other processes	✓	✓	Secured Session Key – Read
xon	Allow messages from other processes	✓	✓	Secured Session Key – Read
zeroize	Zeroize all CSPs	✓		All CSPs – Delete

Table 7 lists the services that are provided on the Line Card platforms.

Table 7 – Mapping of Line Card Specific Services to Roles, CSPs, and Type of Access

Service	Description	Operator		Type of Access
		CO	User	
agents	View console agents	✓	✓	Secured Session Key – Read
btp	Burst Time Plan (BTP) statistics	✓	✓	Secured Session Key – Read
cert_mgr	Certificate Manager command	✓		RSA Private Key – Read/Write RSA Public Key – Read/Write Secured Session Key – Read
da_tunnel	Shows statistics for the tunnel between an external process and the hub line card	✓	✓	Secured Session Key – Read
diagnostic	Diagnostic Command	✓		Secured Session Key – Read
DID	Show modem identification number	✓	✓	Secured Session Key – Read
dumpb	Dump bursts received on hub	✓		Secured Session Key – Read
gige_mon	Gige monitor command	✓	✓	Secured Session Key – Read
hdlc	HDLC Status	✓	✓	Secured Session Key – Read
key_ctrl	Crypto key controller	✓		Dynamic Ciphertext Channel Key – Read/Write
key_mgr	Key manager	✓		Acquisition Ciphertext Channel Key – Read/Write
na_tunnel	Shows the statistics parameters for a tunnel from the hub line card and an external process	✓	✓	Secured Session Key – Read
rx/agc	Rx AGC	✓	✓	Secured Session Key – Read
rx/band	Rx Band	✓	✓	Secured Session Key – Read
rx/ber/stats	BER Stats	✓	✓	Secured Session Key – Read

Service	Description	Operator		Type of Access
		CO	User	
rx/bitrate	Rx BitRate	✓		Secured Session Key – Read
rx/blklen	Rx BlockLength	✓	✓	Secured Session Key – Read
rx/mod	Rx Modulation	✓	✓	Secured Session Key – Read
rx/payloadlen	Rx PayloadLength	✓	✓	Secured Session Key – Read
rx/refclkdac	Rx Ref Clock DAC	✓		Secured Session Key – Read
rx2/demodkick	Rx DemodKick	✓		Secured Session Key – Read
rx2/snr	Rx SNR	✓	✓	Secured Session Key – Read
rx2/tdmlost	Rx tdm lock lost	✓	✓	Secured Session Key – Read
rxdiag/19DCVoltage	19 Volts Supply Monitor	✓	✓	Secured Session Key – Read
rxdiag/inputdcvoltage	Input DC Voltage	✓	✓	Secured Session Key – Read
rxdiag/mcifpower	Multichannel IF Power	✓	✓	Secured Session Key – Read
rxdiag/mcrfpower	Multichannel RF Power	✓	✓	Secured Session Key – Read
standby	Standby Command	✓		Secured Session Key – Read
swbpfll	Software FLL	✓	✓	Secured Session Key – Read
swfll	Software FLL	✓	✓	Secured Session Key – Read
sync_mgr	Check options file sync msg list	✓	✓	Secured Session Key – Read
sync_rsp_mgr	Check response msg list	✓	✓	Secured Session Key – Read
TERMINATE	Kill process	✓	✓	Secured Session Key – Read
tplog	Timeplan Log	✓	✓	Secured Session Key – Read
tunnel	Tunnel control	✓	✓	Secured Session Key – Read

Service	Description	Operator		Type of Access
		CO	User	
tunnel_control	Tunnel controller command	✓	✓	Secured Session Key – Read
tx/band	Tx Band Selection	✓	✓	Secured Session Key – Read
tx/band	Tx Band Select	✓		Secured Session Key – Read
tx/fllref	Tx FLL Ref Clock	✓	✓	Secured Session Key – Read
tx/lock	Tx Lock Status	✓	✓	Secured Session Key – Read
tx/powermode	Tx Power Mode	✓	✓	Secured Session Key – Read
tx/raven	Tx Raven	✓	✓	Secured Session Key – Read
wam	wam	✓	✓	Secured Session Key – Read

Table 8 lists services that are provided on the Evolution e8350 Satellite Router, iConnex e800,iConnex e850MP, iConnex e850MP-INd, and iConnex e850MP-IND with Heat Sink platforms.

Table 8 – Mapping of Remote Platform Specific Services to Roles, CSPs, and Type of Access

Service	Description	Operator		Type of Access
		CO	User	
acq	Enables acquisition debugging	✓	✓	Secured Session Key – Read
ber/stats	BER Stats	✓	✓	Secured Session Key – Read
btp	Tx Debug	✓	✓	Secured Session Key – Read
classifier	Classifier command	✓	✓	Secured Session Key – Read
cpu	Show CPU utilization percentage	✓	✓	Secured Session Key – Read
csp	Enables/disables csp mode	✓		Secured Session Key – Read
dfoe	Dynamic Features and Options Exchange	✓		Secured Session Key – Read
dhcp	DHCP server command	✓	✓	Secured Session Key – Read
dns	DNS control	✓	✓	Secured Session Key – Read

Service	Description	Operator		Type of Access
		CO	User	
dubmpb	Dump bursts received on TDMA Rx2 of the remote	✓		Secured Session Key – Read
dvbs2	dvbs2 st	✓		Secured Session Key – Read
enc	Encryption control command	✓		Secured Session Key – Read
encs	Encryption session control command	✓		Secured Session Key – Read
fake_acq	Fake ACQ control	✓	✓	Secured Session Key – Read
fan/rpm	Fan RPM	✓	✓	Secured Session Key – Read
fan/status	Fan Status	✓	✓	Secured Session Key – Read
fpga/rx1	FPGA Rx1 Driver	✓	✓	Secured Session Key – Read
fpga/rx2	FPGA Rx2 Driver	✓	✓	Secured Session Key – Read
gpspollinterval	seconds	✓	✓	Secured Session Key – Read
gpsvalidationstatus	Status of GPS validation	✓	✓	Secured Session Key – Read
gre	Generic Routine Encapsulation (GRE) protocol	✓	✓	Secured Session Key – Read
icmp	Internet Control Message Protocol (ICMP) inspection layer console command	✓	✓	Secured Session Key – Read
inroute_list	Inroute List	✓	✓	Secured Session Key – Read
ipv4	IPv4 protocol acceleration control layer	✓	✓	Secured Session Key – Read
ktun	Kernel Tunnel Command	✓	✓	Secured Session Key – Read
l2tp_compress	L2TP payload compress	✓	✓	Secured Session Key – Read
lfc	Local	✓	✓	Secured Session Key – Read
ll	Link Layer control	✓	✓	Secured Session Key – Read
mcqos	Multicast QoS	✓	✓	Secured Session Key – Read

Service	Description	Operator		Type of Access
		CO	User	
mesh	Forces the remote out of mesh	✓		Secured Session Key – Read
mesh_marker	mesh_marker layer command	✓	✓	Secured Session Key – Read
meshdebug	Mesh Debug	✓		Secured Session Key – Read
nat	NAT Control	✓	✓	Secured Session Key – Read
offline	Offline	✓	✓	Secured Session Key – Read
online	Online	✓	✓	Secured Session Key – Read
oobc	Out of Band Control layer stats and params	✓		Secured Session Key – Read
ota	Over-The-Air statistics	✓		Secured Session Key – Read
phy	Read PHY status register	✓		Secured Session Key – Read
pm	Pad upper Mux stats	✓		Secured Session Key – Read
powermgmt	Power Management	✓	✓	Secured Session Key – Read
pull_engine	PullDown Engine Control	✓	✓	Secured Session Key – Read
qos	Quality of Service (QoS) control	✓	✓	Secured Session Key – Read
remotestate	Displays the current remote state	✓	✓	Secured Session Key – Read
rmtarp	Mesh ARP table	✓	✓	Secured Session Key – Read
rmtlock	Locks the remote to work in a specific network	✓		Secured Session Key – Read
rmtstat	Toggle printing Remote Status messages	✓	✓	Secured Session Key – Read
rx/cof	Rx Carrier Offset	✓	✓	Secured Session Key – Read
rx/demod	Rx Demod	✓	✓	Secured Session Key – Read

Service	Description	Operator		Type of Access
		CO	User	
rx/demodkick	Rx DemodKick	✓		Secured Session Key – Read
rx/demodsel	Rx Demod Select	✓	✓	Secured Session Key – Read
rx/dvbs2/debug	Sets debug level for Rx dvbs2	✓	✓	Secured Session Key – Read
rx/fastfll	Rx Fast FLL	✓	✓	Secured Session Key – Read
rx/flm	Rx False Lock Monitor	✓		Secured Session Key – Read
rx/gdc	GD Compensation and Monitor	✓	✓	Secured Session Key – Read
rx/griffin	Rx Griffin	✓	✓	Secured Session Key – Read
rx/groundelay	Rx Ground Delay	✓	✓	Secured Session Key – Read
rx/pointing	Rx Pointing	✓		Secured Session Key – Read
rx/snr	Rx SNR	✓	✓	Secured Session Key – Read
rx/stv	STV Support	✓	✓	Secured Session Key – Read
rx/swfll	Software SCPC FLL	✓	✓	Secured Session Key – Read
rx/tdmlost	Rx tdm lock lost	✓	✓	Secured Session Key – Read
rx/ts_stats	Rx Transport Stream Lock Stats	✓		Secured Session Key – Read
rx2/blklen	Rx BlockLength	✓	✓	Secured Session Key – Read
rx2/crc	Rx2 CRC Count	✓	✓	Secured Session Key – Read
rx2/fec	Tx FECRate	✓	✓	Secured Session Key – Read
rx2/meshfsd	Mesh FSD	✓	✓	Secured Session Key – Read
rx2/mod	Rx Modulation	✓	✓	Secured Session Key – Read
rx2/payloadlen	Rx PayloadLength	✓	✓	Secured Session Key – Read

Service	Description	Operator		Type of Access
		CO	User	
rxdiag/14rxanalog	14-Analog-Rx (AIN6)	✓	✓	Secured Session Key – Read
rxdiag/14txanalog	14-Analog-Rx (AIN5)	✓	✓	Secured Session Key – Read
rxdiag/24DCVoltage	24 DC Voltage	✓	✓	Secured Session Key – Read
rxdiag/5DCVoltage	5 DC Voltage	✓	✓	Secured Session Key – Read
rxdiag/consolevoltage	Console Voltage	✓	✓	Secured Session Key – Read
rxdiag/rxvoltage	Rx IFL DC Voltage	✓	✓	Secured Session Key – Read
rxdiag/txcurrent	Tx IFL DC VOltage	✓	✓	Secured Session Key – Read
rxdiag/txpll	Tx PLL VCC (AIN4)	✓	✓	Secured Session Key – Read
rxdiag/txvoltage	Tx IFL DC Voltage	✓	✓	Secured Session Key – Read
rxdiag/vinps	Input Voltage PS (AIN3)	✓	✓	Secured Session Key – Read
sar	Segmentation and Reassembly (SAR) control	✓	✓	Secured Session Key – Read
satmac	Debugs the satellite MAC layer	✓		Secured Session Key – Read
sd	Sar lower Mux stats	✓		Secured Session Key – Read
switch/status	Marvell Switch Status	✓	✓	Secured Session Key – Read
switch/vlans	Marvell Switch VLAN configuration	✓	✓	Secured Session Key – Read
switch/pvid	Marvell Switch Port PVID values	✓	✓	Secured Session Key – Read
switch/fwmap	Marvell Switch Port FW Map	✓	✓	Secured Session Key – Read
switch/power	Marvell Switch Power Control	✓	✓	Secured Session Key – Read
switch/params	Marvell Switch option file params	✓	✓	Secured Session Key – Read
transec_layer	TRANSEC layer command	✓	✓	Secured Session Key – Read

Service	Description	Operator		Type of Access
		CO	User	
tx/10	Tx Pattern 1-0	✓		Secured Session Key – Read
tx/bitrate	Tx Bitrate	✓		Secured Session Key – Read
tx/blklen	Tx BlockLength	✓	✓	Secured Session Key – Read
tx/debug	Tx Debug	✓		Secured Session Key – Read
tx/fecrate	Tx FECRate	✓	✓	Secured Session Key – Read
tx/freq_val	Tx Freq Record Program Values	✓		Secured Session Key – Read
tx/fsd	Tx FSD	✓	✓	Secured Session Key – Read
tx/keyline	Tx Keyline	✓	✓	Secured Session Key – Read
tx/lfo	Tx Local Frequency Offset	✓		Secured Session Key – Read
tx/mod	Tx Modulation	✓	✓	Secured Session Key – Read
tx/payloadlen	Tx PayloadLength	✓	✓	Secured Session Key – Read
tx/power	Tx Power	✓		Secured Session Key – Read
tx/ssb	Tx SSB	✓		Secured Session Key – Read
tx/status	Tx Status	✓	✓	Secured Session Key – Read
tx/tdma/debug	sets debug level for tx tdma	✓	✓	Secured Session Key – Read
tx/tpcblocks	Tx Num of Tpc Blocks Per Frame	✓	✓	Secured Session Key – Read
ucp	Display UCP information	✓	✓	Secured Session Key – Read
udp	UDP Command	✓	✓	Secured Session Key – Read
udp_compress	UDP Payload compress	✓	✓	Secured Session Key – Read
vlan	Virtual Local Area Network (VLAN) control	✓	✓	Secured Session Key – Read

Service	Description	Operator		Type of Access
		CO	User	
wam2	wam	✓	✓	Secured Session Key – Read

Table 9 maps Client User Role services to inputs, outputs and CSPs.

Table 9 – Mapping of Client User Role's Services to Inputs, Outputs, CSPs, and Type of Access

Service	Description	Input	Output	Type of Access
Traffic Routing	Secured traffic routing 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

2.5 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 1 physical security requirements using clear coating over the boards and their physical components to protect against environment and physical damage. The boards will be enclosed in production-grade enclosures for added physical security. A sample enclosure can be seen in Figure 3.

Figure 3 – e8000 Series Enclosure

Figure 4 below show the iConnex e800 Satellite Router Board. Please note that the e800 and e8350 boards have the same appearance; the only difference is that the e8350 has an 8 port Ethernet switch that is mounted to the back of the metal chassis that it fits into.

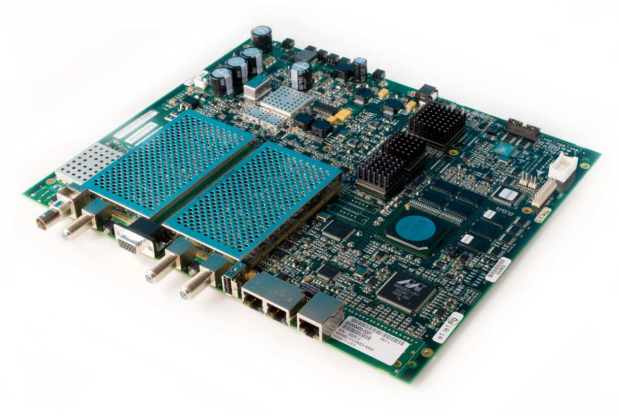

Figure 4 – iConnex e800 Satellite Router Board

Figure 5 below shows the iConnex e850MP Satellite Router Board.

Figure 5 – iConnex e850MP Satellite Router Board

Figure 6 below show the Evolution eM1D1 Line Card. Please note that Evolution eM1D1 and Evolution eM0DM Line Cards have the same appearance.

Figure 6 – Evolution eM1D1 Line Card

2.6 Operational Environment

The modules' firmware, iDX version 2.3.1, 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 itself.

2.7 Cryptographic Key Management

The cryptographic modules implement the FIPS-Approved algorithms shown in Table 10:

Table 10 – FIPS-Approved Algorithm Implementations

Algorithm	Certificate Number
AES[15] in CBC[16] and CFB[17] modes – encrypt/decrypt 256-bit key (Software Implementation)	1944
AES in CBC mode – encrypt/decrypt 256-bit key (Hardware Implementation)	1945

[15] AES – Advanced Encryption Standard
[16] CBC – Cipher-Block Chaining
[17] CFB – Cipher Feedback Mode

Algorithm	Certificate Number
SHA[18]-1	1709
HMAC SHA-1	1173
RSA[19] ANSI X9.31 Key Generation – 2048-bit key	1007
RSA sign/verify – 1024-bit to 2048-bit keys	1007
ANSI[20] x9.31 Appendix A.2.4 Pseudo Random Number Generator (PRNG)	1024

Additionally, the modules utilize the following non-FIPS-Approved algorithm implementation, which are allowed in a FIPS-Approved mode of operation:

- Diffie-Hellman 1024 bits key (PKCS#3, key agreement/key establishment methodology provides 80 bits of encryption strength)
- Non-FIPS Approved PRNG for seeding the ANSI X9.31 PRNG
- RSA 2048 bits key encrypt/decrypt (PKCS#1, key wrapping; key establishment methodology provides 112 bits of encryption strength)
- PBKDF[21] (SP800-132, Non-Approved)

Additional information concerning SHA-1, Diffie-Hellman key agreement/key establishment, RSA key signatures and ANSI X9.31 and specific guidance on transitions to the use of stronger cryptographic keys and more robust algorithms is contained in NIST Special Publication 800-131A.

The modules support the following critical security parameters a described in Table 11.

Table 11 – List of 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	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

[18] SHA – Secure Hash Algorithm
[19] RSA – Rivest, Shamir, and Adleman
[20] ANSI – American National Standards Institute
[21] PBKDF – Password Based Key Derivation Function

Key /Component/ CSP	Key Type	Generation / Input	Output	Storage	Zeroization	Use
Acquisition Ciphertext Channel (ACC) Key	AES-256 CBC key	Externally generated, entered in plaintext 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 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	Exits in plaintext, can be viewed by the Crypto-Officer in plaintext	In flash in plaintext	By global zeroize command	Authenticates TLS channel and transports Global Session Key and Link Encryption Key
RSA Public Key	RSA 2048-bit public key	Internally generated	Exits in plaintext, can be viewed by the Crypto-Officer in plaintext	In flash in plaintext	By global zeroize command	Authenticates TLS channel and transports Global Session Key & 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	1024-bit DH private exponent	Internally generated	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	1024-bit DH public exponent	Internally generated	Exits electronicall y in plaintext form	Resides in volatile memory in plaintex	Zeroized after session is over	Establishes Secured Session Key during SSH or TLS sessions
SSH Authentication Key	HMAC-SHA1	Generated internally	Never exits the module	Stored inside the volatile memory in plaintext, inside the module	By global zeroize command	It is 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

Key /Component/ CSP	Key Type	Generation / Input	Output	Storage	Zeroization	Use
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
ANSI X9.31 PRNG Seed	16 bytes of seed	Independently generated by the non-approved PRNG	Never exits the module	Resides in volatile memory in plaintext	Zeroized after session is over	Seeds the ANSI X9.31 PRNG
ANSI X9.31 PRNG Seed Key	32 bytes of seed key	Independently generated by the non-approved PRNG	Never exits the module	Resides in volatile memory in plaintext	Zeroized after session is over	Seeds the ANSI X9.31 PRNG
HMAC Key	HMAC SHA-1	Internally Generated	Exits in plaintext	Resides in volatile memory in plaintext	Zeroized after session is over	Securely exchange information during SSH session

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 any Application Programming Interface (API) 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 any Application Programming Interface (API) 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 a remote. Each remote uses a different Link Encryption Key. Notice that in the FIPS mode of operation, link encryption without TRANSEC is not allowed.

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 (1024-bit exponent) mechanism. The DH private key is calculated during session initialization and resides only in volatile memory in plaintext. The modules do not provide any API to access the DH private key. The private key is zeroized after the session is over.

The Crypto-Officer and the User enters passwords to request access. The modules store a SHA-1 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 X9.31 PRNG seed and seed keys are generated from the internal non-FIPS Approved PRNG. These values are stored in volatile memory and can be destroyed by powering down the modules.

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 transitions to an error state in which all interfaces except the console port 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.

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 a RSA digital signature
- Known Answer Tests (KATs)
  - AES CBC 256-bit key KAT for encrypt/decrypt (FPGA)
  - AES CFB 256-bit key KAT for encrypt/decrypt (Firmware)
  - Triple-DES CBC KAT for encrypt/decrypt[22]
  - RSA KAT for sign/verify
  - X9.31 PRNG KAT

The modules do not perform an independent SHA-1 KAT. The full functionality of the SHA-1 implementation is tested as part of the modules' firmware integrity test, which uses a FIPS-Approved RSA digital signature verification mechanism.

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

2.8.2 Conditional Self-Tests

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

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

2.9 Design Assurance

VT iDirect utilizes Concurrent Versioning Systems (CVS) for its version control system. VT iDirect maintains a unique branch for each major release and on occasion creates branches for special or experimental releases. The FIPS-specific version of VT iDirect firmware is maintained on a dedicated branch, with strict controls on any modification. VT iDirect refers to its entire firmware package as iDX. VT iDirect maintains all project software, configuration files, documentation, FPGA code, bill of material), 3rd party software, and 3rd party binary executables within its Configuration Management system.

Additionally, Microsoft Visual SourceSafe version 6.0 was used to provide configuration management for the modules' FIPS documentation. A revision history is maintained by Visual SourceSafe.

2.10 Mitigation of Other Attacks

This section is not applicable. The modules do not claim to mitigate any attacks beyond the FIPS 140-2 Level 1 requirements for this validation.

3 Secure Operation

The Secure Satellite Broadband Solutions meet overall Level 1 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. For any questions or if issues arise at any point during the installation, configuration, and daily operation of the modules, contact the 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 locally over the console port or remotely over a secured session. Remote secured sessions are provided via TLS, SSH, or the satellite channel.

3.1.1 Initialization

While the modules are shipped with the Linux OS configured for single user mode, they must be configured for use in a TRANSEC-enabled network using a TRANSEC-enabled Protocol Processor and the iBuilder application. All network elements that subsequently created under a TRANSEC-enabled protocol processor will become part of the TRANSEC-compliant network.

This process involves configuring each respective module in iBuilder (entering the device type, serial number, Satellite and LAN[23] IP addresses, db threshold, etc.), uploading the resulting "options file", issuing the Certificate Authority (CA) via the CA Foundry utility in the Network Management Server (NMS), un-checking the "Disable Authentication" option in iBuilder and finally re-uploading the new options file and resetting each module. The resulting TRANSEC-enabled network operates in 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 detailed in the *iDirect Network Management System iBuilder's User Guide*.

The Crypto-Officer should monitor the modules' status by regularly checking the Statistics log information. If any irregular activity is noticed or the module is consistently having errors, then iDirect Technologies customer support should be contacted.

3.1.2 Management

According to FIPS 140-2 requirements, the operating system of the modules must be configured in the single user mode. For a Linux operating system to be in the single user mode, it must meet the following requirements:

- All login accounts except "root" should be removed.
- Network Information Service (NIS) and other named services for users and groups need to be disabled.
- All remote login, remote command execution, and file transfer daemons should be turned off.

iDirect follows the following procedures to configure Linux operating system in single user mode:

1. Log in as the "root" user.

[23] LAN – Local Area Network

2. Edit the system files /etc/passwd and /etc/shadow and remove all the users except “root” and the pseudo-users. Make sure the password fields in /etc/shadow for the pseudo-users are either a star (*) or double exclamation mark (!!). This prevents login as the pseudo-users.
3. Edit the system file /etc/nsswitch.conf and make “files” the only option for “passwd”, “group”, and “shadow”. This disables NIS and other name services for users and groups.
4. Reboot the system for the changes to take effect.

When the modules are received by the Crypto-Officer, the Linux operating system has already been configured in the single user mode. It is suggested that the Crypto-Officer confirm that the above steps have been taken in order to ensure that the operating system is in fact running in single user mode.

By default the modules are not usable in the network. In order to initialize the modules, the Crypto-Officer must define the modules in their iBuilder under a TRANSEC enabled protocol processor and generate options for the modules. For detailed information on initialization, please refer to the *iDirect Network Management System iBuilder's User Guide*.

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, Table 7, and Table 8 for a list of commands available to the User role.

3.3 Client User Guidance

The Client User role utilizes the modules’ traffic routing services. The Client User role is implicitly assumed by a network device or application routing traffic through the modules. There are no special instructions for the Client User to use the modules securely. The Client User should make sure the network is configured with TRANSEC feature (i.e. the FIPS mode of operation) before participating in the network.

4 Acronyms

Table 12 lists all of the acronyms used throughout this document.

Table 12 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
API	Application Programming Interface
BNC	Bayonet Neill-Concelman connector
BUC	Block Up-Converter
CA	Certificate Authority
CBC	Cipher Block Chaining
CFB	Cipher Feedback Mode
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CPU	Central Processing Unit
CSEC	Communications Security Establishment Canada
CSP	Critical Security Parameter
CVS	Concurrent Versioning System
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
ICMP	Internet Control Message Protocol
IP	Internet Protocol
KAT	Known Answer Test
LAN	Local Area Network
LC	Line Card
LED	Light Emitting Diode
LNB	Low Noise Block

Acronym	Definition
MAC	Media Access Control
MHz	Mega Hertz
MUX	Multiplexer
NIS	Network Information Service
NIST	National Institute of Standards and Technology
NMS	Network Management Server
OOB	Out of Band
OS	Operating System
PCB	Printed Circuit Board
PCI	Peripheral Component Interconnect
PKCS	Public Key Cryptography Standard
PRNG	Pseudo Random Number Generator
QoS	Quality of Service
RF	Radio Frequency
RJ	Registered Jack
RS-232	Recommended Standard 232
RSA	Rivest Shamir and Adleman
Rx	Receiver Coaxial Connector
SHA	Secure Hash Algorithm
SMA	SubMiniature version A
SSH	Secure Shell
TDES	Triple Data Encryption Standard
TDMA	Time Division Multiple Access
TLS	Transport Layer Security
TRANSEC	Transmission Security
Tx	Transmitter Coaxial Connector
ULC	Universal Line Card
VPN	Virtual Private Network

Prepared by:
Corsec Security, Inc.

13135 Lee Jackson Memorial Hwy, Suite 220
Fairfax, VA 22033
United States of America

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