iDirect Technologies

Secure Satellite Broadband Solutions

with iDS versions 7.1.2 (7350 iNFINITI Satellite Router; iConnex-700; iConnex-100; and M1D1-T ULC) and 7.1.3 (8350 iNFINITI Satellite Router)

FIPS 140-2
Non-Proprietary Security Policy

Level 1 Validation

Document Version 2.2

Prepared for:

iDirect Technologies
13865 Sunrise Valley Drive
Herndon, VA 20171
Phone: (866) 345-0983
Fax: (703) 648-8014
http://www.idirect.net

Prepared by:

Corsec Security, Inc.
10340 Democracy Lane, Suite 201
Fairfax, VA 22030
Phone: (703) 267-6050
Fax: (703) 267-6810
http://www.corsec.com

Revision History

Version	Modification Date	Modified By	Description of Changes
0.1	2006-11-22	Rumman Mahmud	Initial draft.
0.2	2007-02-15	Rumman Mahmud	The cryptographic module is considered as a hardware module.
0.3	2007-03-22	Rumman Mahmud	Cryptographic module's name changed and added iConnex-100 information.
0.4	2007-04-02	Rumman Mahmud	Inserted algorithm certificate numbers.
0.5	2007-05-18	Xiaoyu Ruan	Revised according to Lab's comments.
0.6	2007-05-22	Xiaoyu Ruan	Revised according to Lab's comments.
0.7	2007-06-01	Xiaoyu Ruan	Revised according to Lab's comments.
0.8	2007-06-04	Xiaoyu Ruan	Added the "Client User" role.
0.9	2007-06-06	Xiaoyu Ruan	Key management changed.
1.0	2007-06-08	Xiaoyu Ruan	Crypto-Officer initialization changed.
1.1	2007-06-14	Xiaoyu Ruan	Reordered service list. Changed Crypto-Officer descriptions.
1.2	2007-06-15	Xiaoyu Ruan	Minor changes.
1.3	2007-06-18	Xiaoyu Ruan	Updated Table 8.
1.4	2007-06-19	Xiaoyu Ruan	Addressed final comments from Lab.
1.5	2007-06-19	Xiaoyu Ruan	Secured Session Key is established only using Diffie-Hellman.
2.0	2007-06-20	Xiaoyu Ruan	Release version.
2.1	2007-12-06	Xiaoyu Ruan	Change Letter.
2.2	2008-02-01	Xiaoyu Ruan	Revised according to Lab's comments.

Table of Contents

Table of Figures

Table of Tables

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Secure Satellite Broadband Solutions from iDirect Technologies. This Security Policy describes how the Secure Satellite Broadband Solutions with iDS version 7.1.2 (applicable to the following hardware: 7350 iNFINITI Satellite Router, Part #9130-0062-0002; iConnex-700, Part #9101-2040-0201; iConnex-100, Part #9101-2040-0202; and M1D1-T ULC, Part #9101-0040-0008) and iDS version 7.1.3 (applicable to the following hardware: 8350 iNFINITI Satellite Router, Part#9100-0040-0013) meet the security requirements of FIPS 140-2 (Federal Information Processing Standards Publication 140-2 – *Security Requirements for Cryptographic Modules*) and how to run the module in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 1 FIPS 140-2 validation of the module.

FIPS 140-2 details the U.S. 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) Cryptographic Module Validation Program (CMVP) website at: http://csrc.nist.gov/groups/STM/cmvp/index.html.

The Secure Satellite Broadband Solutions are referred to in this document as the *cryptographic modules*, the *hardware modules*, or the *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 iDirect website (http://www.idirect.net) contains information on the full line of products from iDirect.
- The CMVP website (http://csrc.nist.gov/groups/STM/cmvp/index.html) contains contact information for answers to 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 Machine
- Other supporting documentation as additional references

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

2 Secure Satellite Broadband Solutions

2.1 Overview

An iDirect Time Division Multiple Access (TDMA) network is composed of a single outroute Single Channel Per Carrier (SCPC) and multiple inroute TDMA carriers. The 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 iDirect's Network Management System that provides configuration and monitoring functions. The iDirect network components consist of the network management server, protocol processor, Hub Line Card (also known as Universal Line Card), and the Ethernet switch with remote modem. In a star topology, the protocol processor acts as the central network controller, the Universal Line Card (ULC) is responsible for the hub side modulation and demodulation (modem) functions, and the remote modem provides modem functionalities for the Ethernet switch.

iDirect's Transmission Security (TRANSEC) feature enables encryption to all Data Link Layer traffic flowing between the ULC and Remote modem using Advanced Encryption Standard (AES). The hardware modules provide TRANSEC features to the TDMA network. The module encrypts the layer 2 traffic with a single global AES 256 key, common to all components. Authentication and key distribution information is protected with Rivest Shamir Adlemann (RSA) 2048 using X.509 certificates. A common deployment of the iDirect network components is shown below.

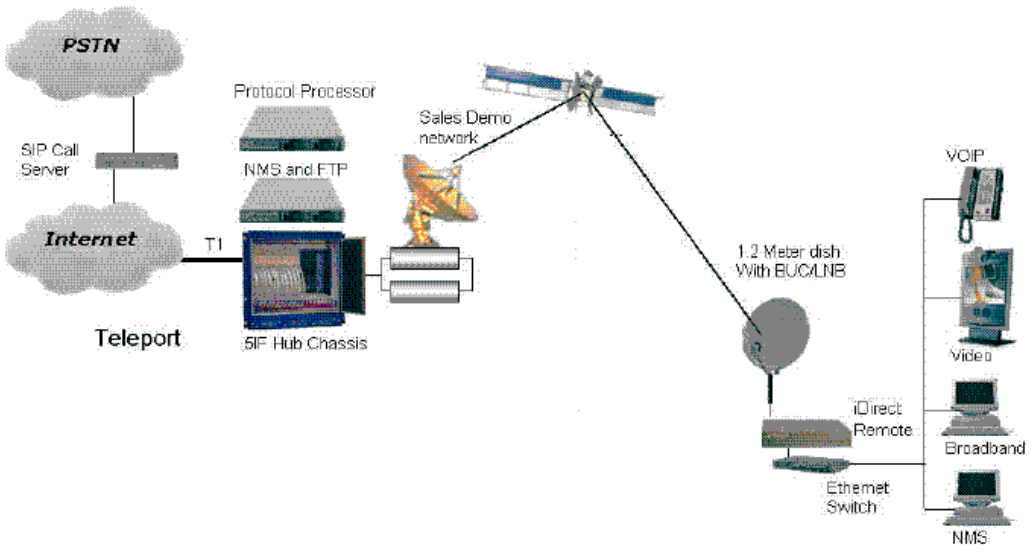

Figure 1 - iDirect Network Deployment

TRANSEC is managed by software. One key set is created for the entire network. All participants of the network then share the key set. Encryption of data occurs in FPGA 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 members of the network can receive and decrypt all data. TRANSEC makes a particular effort to prevent traffic analysis by outside parties.

Link Encryption occurs completely in software. Each remote and its counterpart layer in the protocol processor creates a transmit key (Link Encryption Key, See Table 8) 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 sources and destination link addresses is not encrypted. Broadcast and multicast traffic is not encrypted either. Therefore, link level information, such as HDLC destinations, is not protected by Link Encryption.

The cryptographic modules, known as the Secure Satellite Broadband Solutions, provide the secured traffic routing services. The hardware module runs Linux version 2.4.24-uc0-iDirect0 operating system. The platforms for the cryptographic module are Printed Circuit Boards (PCBs) for the 8350 iNFINITI Satellite Router (Part#9100-0040-0013), 7350 iNFINITI Satellite Router (Part #9130-0062-0002), iConnex-700 (Part #9101-2040-0201), iConnex-100 (Part #9101-2040-0202), and M1D1-T ULC (Part #9101-0040-0008). 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	Roles, Services, and Authentication	1
4	Finite State Model	1
5	Physical Security	1
6	Operational Environment	1
7	Cryptographic Key Management	1
8	Electromagnetic Interference (EMI) / Electromagnetic Compatibility (EMC)	1
9	Self-tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A

2.2 Module Interfaces

The Cryptographic boundaries of the modules are the iDirect PCBs that run the iDS software, which is referred to as “falcon”. Per FIPS 140-2 terminology, the Secure Satellite Broadband Solutions are multi-chip embedded modules that meets 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 blue broken line.

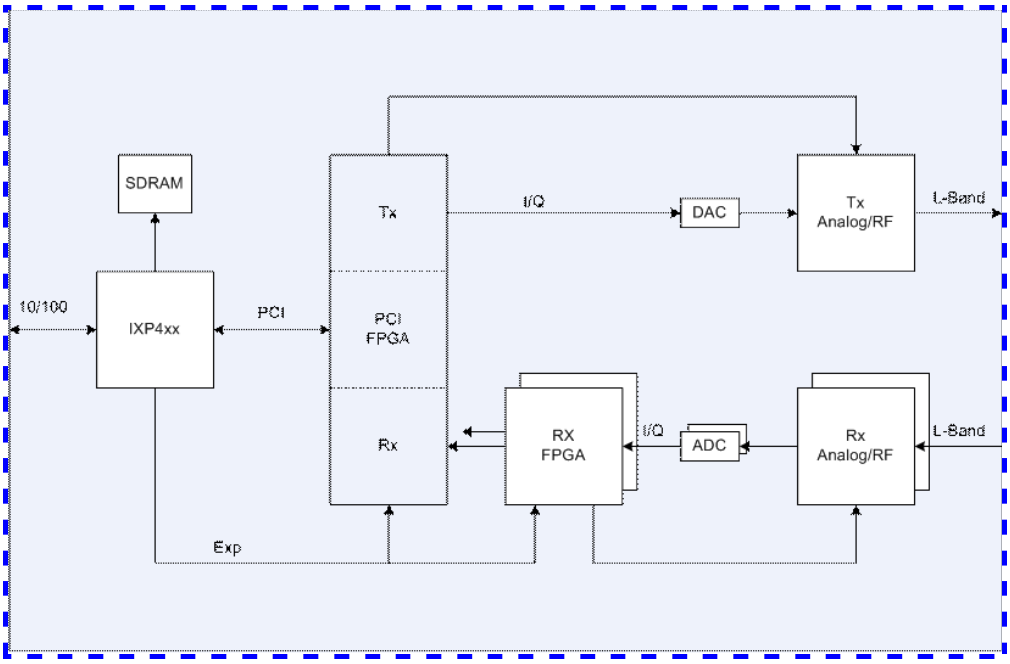

Figure 2 - Cryptographic Module Block Diagram

Physical ports do not differ on different platforms to be validated. The following is a list of the physical ports for the modules that are enabled in the FIPS mode of operation:

- Receiver Coaxial Connector (Rx)
- Transmitter Coaxial Connector (Tx)
- Power connector
- 10/100 Ethernet ports (RJ45)
- One console port (serial over an RJ45)
- Light Emitting Diodes (LEDs)

The 7350 iNFINITI Satellite Router has two (2) additional Ethernet ports marked “ICC In” and “ICC Out” that are disabled in firmware and software. These additional ports are not present on the 8350 iNFINITI Satellite Router.

For the iConnex-700, iConnex-100, and M1D1-T ULC, the choice of how to display the LEDs is determined by the integrator of the PCBs. The LED functions are handled by the falcon application. For the 8350 iNFINITI Satellite Router and 7350 iNFINITI Satellite Router, the meanings of LEDs are defined as follows.

- The Power LED indicates whether the unit is powered On or Off.
- The Status LED indicates the unit’s overall status.
- The Network LED indicates the unit’s network acquisition status.
- The Tx LED indicates the unit’s transmitter status.
- The Rx LED indicates the unit’s receiver status.

The 7350 iNFINITI Satellite Router has two (2) Ethernet ports marked “ICC In” and “ICC Out” that are disabled in firmware and software.

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 2 - FIPS 140-2 Logical Interfaces

FIPS 140-2 Logical Interface	Secure Satellite Broadband Solutions Port/Interface
Data Input	Rx, Ethernet ports
Data Output	Tx, Ethernet ports
Control Input	Rx, Ethernet ports, console port
Status Output	Tx, Ethernet ports, console port, LEDs (8350 iNFINITI Satellite Router and 7350 iNFINITI Satellite Router only)
Power	Power connector

2.3 Roles and Services

The module supports role-based authentication. There are three roles in the module that operators may assume: Crypto-Officer role, User role, and Client User role.

2.3.1 Crypto-Officer Role

The Crypto-Officer role is implicitly assumed when performing installation, configuration and monitoring services for the module. The Crypto-Officer accesses the module 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 module by directly connecting through the console port (RJ45 over Serial port). The Crypto-Officer has to authenticate with account name “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”).
- Remote Command Line Interface (CLI) – The module can be configured and monitored over a remote CLI management interface using Secure Shell (SSH). The Crypto-Officer authenticates with a password to access any services. The module performs a Diffie-Hellman (DH) key agreement mechanism to initialize the SSH session.
- Management Interface over Transport Layer Security (TLS) – The module can also be configured and monitored using a Graphical User Interface (GUI) over a TLS session, such as the iBuilder and iMonitor applications which require a user name and password for access. The module performs RSA authentication and key transport during the TLS handshake (the Crypto Officer password is not required).
- Management over Satellite – Over the satellite channel, the module 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 sent Layer 2 Reset messages when prompted to do so by a password authenticated user.

Telnet is not an external interface, but it is available internal to the Linux operating system. On the console, in order to login as “admin”, the Crypto-Officer has to first log into the Linux operating system using the “root” account and the applicable password and then telnet to the localhost (telnet 0). The Crypto-Officer must then enter “admin” and the password at the prompt.

When the Crypto-Officer accesses the module via SSH, he is able to bypass the “root” authentication and logs into the CLI interface directly with the “admin” account and the appropriate password.

Table 3, Table 4, and Table 5 list all CLI services for to a Crypto-Officer. The services available to the User role (see Figure 3) are also available to a Crypto-Officer.

The CLI services can be categorized in three different groups:

1. General Services: Common functions to the iDS software.

2. Hub Specific Services: These services are only accessible on the M1D1-T ULC platform.

3. Remote Specific Services: Services specific to the 8350 iNFINITI Satellite Router, 7350 iNFINITI Satellite Router, iConnex-700, and iConnex-100 platforms.

Crypto-Officer enters commands with the appropriate parameters to access the services of the module and the module outputs the command response. Descriptions of the services available to the Crypto-Officer role 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 3 - Mapping of Crypto-Officer Role's General Services to CSPs and Type of Access

Service	Description	CSP and Type of Access
arp	Address Resolution Protocol (ARP) control	Secured Session Key – Read
cpu	Show Central Processing Unit (CPU) utilization percentage	Secured Session Key – Read
csp	enable/disable csp mode	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) status	Secured Session Key – Read
dumpb	Dumps bursts received on hub	Secured Session Key – Read
ENTER_ERROR_STATE	Enter Error state	Secured Session Key – Read
eth	Configure a network interface	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
hdlc	HDLC stats	Secured Session Key – Read
hookstatus (not available in FIPS mode)	Protocol hookup status	Secured Session Key – Read
igmp	Multicast control	Secured Session Key – Read
ip	Router control	Secured Session Key – Read
keyroll_mgr	Keyroll manager command	Global Session Key – Read/Write Secured Session Key – Read
mac	Media Access Control (MAC) control	Secured Session Key – Read
mux (not available in FIPS mode)	Multiplexer (MUX) Table Dump	Secured Session Key – Read
netstat	Checks network configuration and activity	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
params	View/edit global parameters	Secured Session Key – Read
pasoc	Command for the packet socket layer	Secured Session Key – Read
passwd	Change password	Password - Write Secured Session Key – Read
pcmd	Periodic console Command	Secured Session Key – Read

Service	Description	CSP and Type of Access
peek	Raw memory read - can be dangerous	Secured Session Key – Read
ping	Ping Utility	Secured Session Key – Read
poke	Raw memory write - can be dangerous	Secured Session Key – Read
service	Service start/stop command	Secured Session Key – Read
status	show status of stack	Secured Session Key – Read
systray	Debugs systray messages (mulicast messages sent on the Local Access Network or LAN)	Secured Session Key – Read
timer	Timer 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
transec_layer	Management command for the protocol layer which communicates packet by packet instructions to the FPGA firmware	Secured Session Key – Read
uptime	System and application uptime	Secured Session Key – Read
x509	Manage X509 Certificates and RSA keys	X.509 Certificate - Read/Write Secured Session Key – Read
zeroize	Zeroize all CSPs	All CSPs – Delete

Table 4 lists Crypto-Officer services that are provided on the M1D1-T ULC platform only.

Table 4 - Mapping of Crypto-Officer M1D1-T Platform Specific Services to CSPs and Type of Access

Service	Description	CSP and Type of Access
cert_mgr	cert manager command	X.509 Certificate – 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
na_tunnel	Shows the statistics parameters for a tunnel from the hub line card and an external process	Secured Session Key – Read
standby	Standby Command	Secured Session Key – Read
tplog	Timeplan Log	Secured Session Key – Read
tunnel	Tunnel control	Secured Session Key – Read
tunnel_control	Tunnel controller command	Secured Session Key – Read

Table 5 lists Crypto-Officer services that are provided on the 8350 iNFINITI Satellite Router, 7350 iNFINITI Satellite Router, iConnex-700, and iConnex-100 platforms.

Table 5 - Mapping of Crypto-Officer Remote Platform Specific Services to CSPs and Type of Access

Service	Description	CSP and Type of Access
acq	Enables acquisition debugging	Secured Session Key – Read

Service	Description	CSP and Type of Access
csp	enable/disable csp mode	Secured Session Key – Read
delay	Usage: delay <msecs to sleep>	Secured Session Key – Read
dhcp	DHCP server command	Secured Session Key – Read
enc	Encryption control command	Secured Session Key – Read
encs	Encryption session control command	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
ipv4	IPv4 protocol acceleration control layer	Secured Session Key – Read
ktun	Kernel Tunnel Command	Secured Session Key – Read
ll	Link Layer control	Secured Session Key – Read
mesh	Forces the remote out of mesh	Secured Session Key – Read
meshdebug	Mesh Debug	Secured Session Key – Read
oob	OOB control	Secured Session Key – Read
ota	Over-The-Air statistics	Secured Session Key – Read
pad	Packet Assembler Disassembler (PAD) control	Secured Session Key – Read
qos	QoS control	Secured Session Key – Read
remotestate	Displays the current remote state	Secured Session Key – Read
rlock	Locks the remote to work in a specific network	Secured Session Key – Read
rmtarp	Mesh ARP table	Secured Session Key – Read
rmtstat	Toggle printing Remote Status messages	Secured Session Key – Read
phy	read physical layer status register	Secured Session Key – Read
pm	Pad upper Mux stats	Secured Session Key – Read
sar	Segementation 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
spoof	Spoof Command	Secured Session Key – Read
systray	Debugs systray messages (mulicast messages sent on the Local Access Network or LAN)	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

2.3.2 User Role

The User has the ability to access the falcon console over the satellite network.

On the console, the User is authenticated with account name “user” or “diagnostic” and a password to access any services. In order to login as “user” or “diagnostic”, the User has to first log into the Linux operating system with the “root” account and the applicable password and then telnet to the localhost (telnet 0). The User must then enter

"user" or "diagnostic" and the appropriate password at the prompt. Accounts "user" and "diagnostic" employ the same password authentication 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 6 - Mapping of User Role's Services to Inputs and Outputs

Service	Description	Input	Output
DID	Show identification number	Command	Identification number
sn	Show modem serial number	Command	Serial number
clear	Clear screen	Command	Screen cleared
eloop	Display event loop status	Command	Event loop status
reset	Reset machine or service	Command	Command status
packages	Get detailed installed package information	Command	Package information
ps	Report the process status	Command	Process status
version	Get build information	Command	Build information
mem	Get resource information	Command	Resource information
heap	Get memory usage information	Command	Memory usage
laninfo	View IP address/netmask	Command	IP address and netmask
latlong	Report Global Positioning System (GPS) information of a locally attached GPS device, if one is present.	Command	GPS information of a locally attached GPS devic
versions_report	Display full operating environment report	Command	Full operating environment report

2.3.3 Client User Role

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

Table 7 - Mapping of Client User Role's Services to Inputs, Outputs, CSPs, and Type of Access

Service	Description	Input	Output	CSP and Type of Access
Traffic Routing	Secured traffic routing at the data-link layer	Data Link layer packet	Data Link layer packet	Global Session 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	No

2.4 Physical Security

The Secure Satellite Broadband Solutions are multi-chip embedded cryptographic modules per FIPS 140-2 terminology. For the 8350 and 7350 routers, the platform is a PCB that is surrounded by a metal case entirely enclosing the internals of the module and the case itself is removable using screws or hand screws. The 8350 router shown in Figure 3 and the 7350 router shown in Figure 4 are being validated as multi-chip embedded modules for level 1.

Figure 3 - 8350 iNFINITI Satellite Router

Figure 4 - 7350 iNFINITI Satellite Router

700-T iNFINITI iConnex, iConnex-100, and M1D1-T Universal Line Card are PCBs that consist of production grade components and are validated as multi-chip embedded modules.

Figure 5 - 700-T iNFINITI iConnex and M1D1-T Universal Line Card

iConnex-100, shown in Figure 6 below, is very similar to 700-TiNFINITI iConnex.

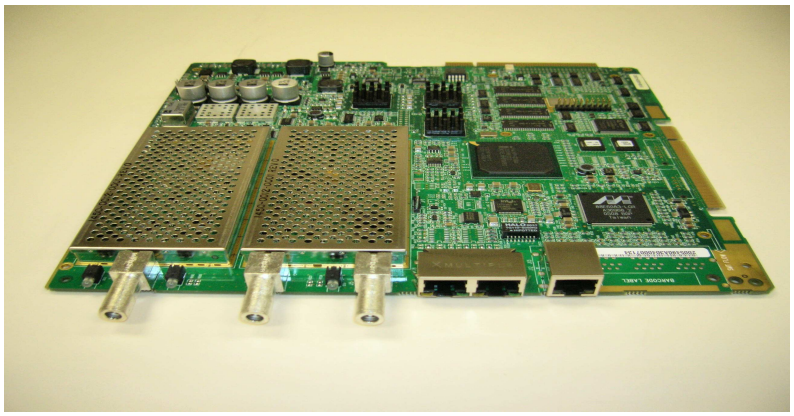

Figure 6 - iConnex-100

2.5 Operational Environment

The module is installed in its compiled form as an executable software running on customized Linux version 2.4.24-uc0-iDirect0. The operating system protects memory and process space from unauthorized access. The software integrity test protects against unauthorized modification of the module itself.

2.6 Cryptographic Key Management

The cryptographic module implements the following FIPS-approved algorithms:

- AES in CBC and CFB modes – encrypt/decrypt 256-bit key (certificate 527, 528)
- TDES in CBC mode – encrypt/decrypt 1, 2, 3 keying options (certificate 534)
- SHA-1 – FIPS 180-2 (certificate 600)
- PRNG – American National Standards Institute (ANSI) X9.31 Appendix A.2.4 (certificate 303)
- RSA – signature verification 2048-bit key (certificate 238)

The cryptographic module implements the following FIPS-approved key agreement/key establishment technique:

- Diffie-Hellman 1024 bits key (PKCS #3, key agreement/key establishment methodology provides 80 bits of encryption strength)

Additionally, the module utilizes the following non-FIPS-approved algorithm implementation:

- Non-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)

The module supports the following critical security parameters:

Table 8 - List of Cryptographic Keys, Cryptographic Key Components, and CSPs

Key/Component/CSP	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 software integrity check during power-up and upgrade

Key/Component/CSP	Type	Generation / Input	Output	Storage	Zeroization	Use
Global Session 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
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	Never exits the module, but 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 and Link Encryption Key
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
Crypto-Officer Password	Password	Entered in plaintext	Never exits the module	Hash value of the password is stored in flash	By global zeroize command	Authenticates the 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	Authenticates the User role
ANSI X9.31 PRNG Seed and Seed Key	16 bytes of seed and 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

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

Global Session keys are AES CBC 256-bit keys that are used to encrypt/decrypt routing traffic flowing across the satellite network. AES cipher operation using Global Session 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 (RSA key transport). The module does not provide any Application Programming Interface (API) access to the Global Session 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 Secure Session Key is generated internally during DH key agreement. Cipher operation for the secured management interface is done in a software implementation of the module. The AES key is stored only in volatile memory and is zeroized after the session is over.

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 module and is used for TLS authentication and 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, which includes logging into "root" with the appropriate password.

The module performs 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 module does 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 authenticate with passwords. The module stores a SHA-1 based hash value for each password onto the flash and never outputs it. The hash value can be zeroized by using the module's zeroization command.

The X9.31 PRNG seed and seed keys are generated from the internal FIPS non-approved PRNG. These values are stored in volatile memory and can be destroyed by powering down the module.

2.7 Self-Tests

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

- Software integrity check using a RSA digital signature
- Known Answer Tests (KATs)
    - AES CBC 256-bit key KAT for encrypt/decrypt
    - Triple-DES CBC KAT for encrypt/decrypt
    - RSA KAT for sign/verify
    - HMAC-SHA-1 KAT
    - X9.31 PRNG KAT

The module does not use HMAC-SHA-1. The KAT for HMAC-SHA-1 is intended to test SHA-1.

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

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

If any of the power-up self-tests fail, the module writes an indicator message in the Event log. In this state all interfaces except the console port are disabled. The Crypto-Officer may execute on demand self-tests by resetting the module or cycling the module's power.

2.8 Design Assurance

iDirect utilizes Concurrent Versioning Systems (CVS) for its version control system. iDirect maintains a unique branch for each major release and on occasion creates branches for special or experimental releases. The FIPS-specific version of iDirect software is maintained on a dedicated branch, with strict controls on any modification. iDirect refers to its entire software package as iDS. 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 module's FIPS documentation. A revision history is maintained by Visual SourceSafe.

2.9 Mitigation of Other Attacks

No claims are made that the modules mitigate any attacks beyond the FIPS 140-2 Level 1 requirements for this validation.

3 Secure Operation

The Secure Satellite Broadband Solutions meet Level 1 requirements for FIPS 140-2. The sections below describe how to place and keep the module in a FIPS-approved mode of operation.

3.1 Crypto-Officer Guidance

The Crypto-Officer is responsible for installing, configuring, and monitoring the module. The Crypto-Officer accesses the module 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 are 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 IP addresses, db threshold, etc.), uploading the resulting 'options file', issuing the Certificate Authority 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.

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 module's 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 module 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.
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 module is 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 module is not usable in the network. In order to initialize the module, the Crypto-Officer must define the module in their iBuilder under a TRANSEC enabled protocol processor and generate options for the module. 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 module over the satellite network and execute certain commands that are not security-relevant. See Table 6 for a list of commands available to the User role.

3.3 Client User Guidance

The Client User role utilizes the module's traffic routing services. The Client User role is implicitly assumed by a network device or application routing traffic through the module. There are no special instructions for the Client User to use the module 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 9 - Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
API	Application Programming Interface
CA	Certification Authority
CBC	Cipher Block Chaining
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CPU	Central Processing Unit
CSP	Critical Security Parameter
CVS	Concurrent Versioning Systems
DH	Diffie-Hellman
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
FPGA	Field Programmable Gate Array
GPS	Global Positioning System
HDLC	High-level Data Link Control
HMAC	Hash Message Authentication Code
ICMP	Internet Control Message Protocol
IP	Internet Protocol
KAT	Known Answer Test
LAN	Local Access Network
LED	Light Emitting Diode
MAC	Media Access Control
MUX	Multiplexer
NIS	Network Information Service
NIST	National Institute of Standards and Technology
OOB	Out of Band
PCB	Printed Circuit Board
PRNG	Pseudo Random Number Generator
RSA	Rivest, Shamir, and Adleman
Rx	Receive Coaxial Connector
SCPC	Single Channel Per Carrier
SHA	Secure Hash Algorithm

Acronym	Definition
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