NetModem II Plus v5.0
(Hardware Version 5.0,
Firmware Version 5.0.1)

FIPS 140-2 Non-Proprietary Security Policy

Level 1 Validation
Version 1.00

July 2004

Table of Contents

List of Tables

List of Figures

INTRODUCTION

Purpose

This is the non-proprietary Cryptographic Module Security Policy for the NetModem II Plus v5.0 from iDirect Technologies (iDirect). This security policy describes how the NetModem II Plus v5.0 meets the security requirements of FIPS 140-2 and how to operate 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 (Federal Information Processing Standards Publication 140-2 — *Security Requirements for Cryptographic Modules*) 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/cryptval/.

The NetModem II Plus v5.0 is referred to in this document as the NetModem II Plus, the NetModem II+, the NetModem, or the module.

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 Technologies website (http://www.idirect-tech.com/) contains information on the full line of products from iDirect.
- The CMVP website (http://csrc.nist.gov/cryptval/) contains contact information for answers to technical or sales-related questions for the module.

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.

NETMODEM II PLUS

Overview

There is a huge demand for high-speed broadband TCP/IP communications. This is especially true in remote locations where conventional land-based solutions are not available, or are not cost-effective. iDirect Technologies provides solutions that allow enterprises of any size, in virtually any location, to access broadband TCP/IP communications via satellite. Our technology provides the flexibility, capability, and reliability that enterprise and government customers need to support critical business applications.

The iDirect Broadband VSAT Network System is an advanced TCP/IP communications system that enables high-speed bandwidth-on-demand networking within a star or point-to-point topology. The system is fully integrated with iDirect's Network Management System that provides configuration and monitoring functions. The iDirect network components consist of the Protocol Processor, Hub Line Card, and the NetModem II+ remote. In a star topology, the Protocol Processor acts as the central network controller, the Hub Line Card is responsible for the hub side modulation and demodulation functions, and the NetModem II+ provides all remote network access functions such as TCP acceleration and encryption. Two NetModems may also be set up in a direct point-to-point configuration for back-haul applications.

In an iDirect TCP/IP network, traffic is optimized for satellite transmission, squeezing the maximum performance out of the bandwidth provided by satellite links. All IP traffic flowing between the NetModems or the Protocol Processor and NetModems is encrypted using Triple-DES.

Module Interfaces

The NetModem II Plus is a multi-chip standalone cryptographic module that meets overall FIPS 140-2 Level 1 requirements. The cryptographic boundary of the NetModem is the metal case, which completely encloses the module.

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	N/A
7	Cryptographic Key Management	1
8	EMI/EMC	3
9	Self-tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A

Table 1 – Security Level Per FIPS 140-2 Section

The NetModem has two receiver coaxial connectors (RX IF), one transmitter coaxial connector (TX IF), one power connector, one 10/100 Ethernet port (RJ45), one console port (serial over an RJ45), and eleven light emitting diodes (LEDs – three in the front, eight in the rear). These physical ports are depicted in the following figure:

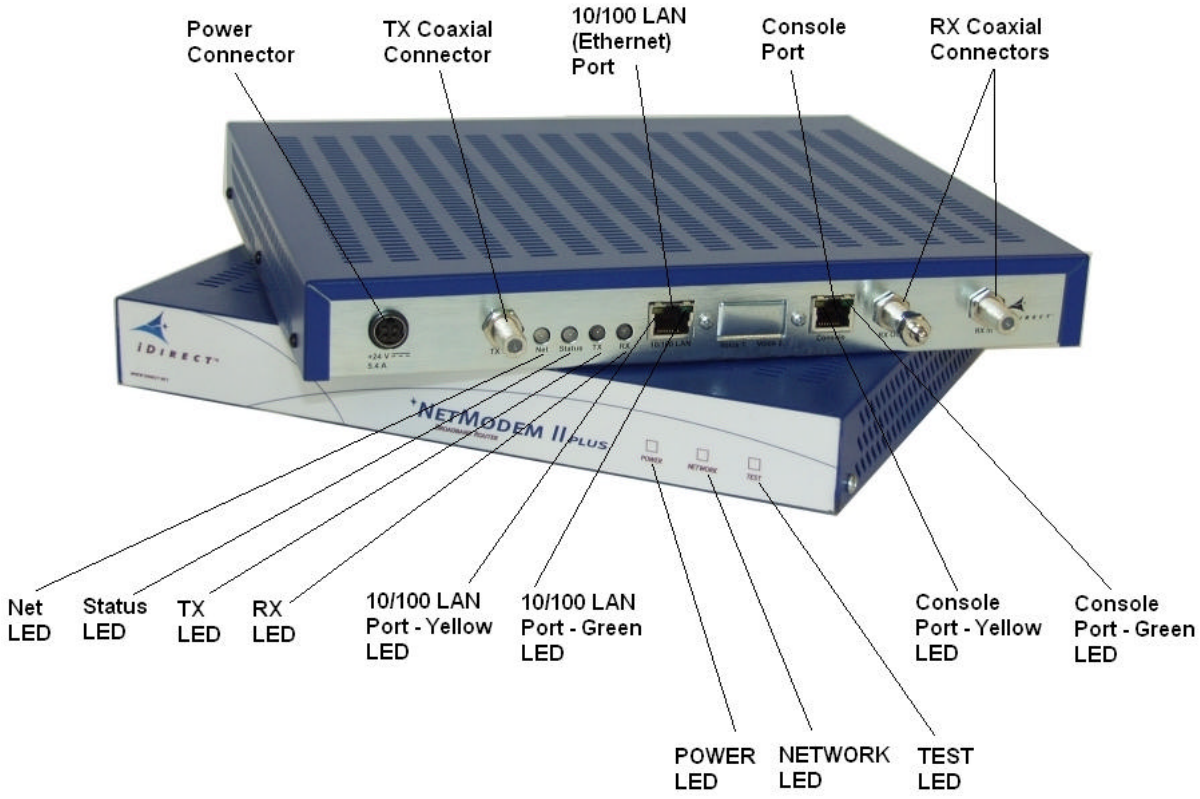

Figure 1 – Front and Rear Physical Ports

The multi-colored LEDs provide status indication for the NetModem, as detailed in the following tables:

LED	Status Indication	Status Description
Power	Green	Unit is powered on.
All	All briefly lit	Unit's bootloader is starting
Network	Flashing Yellow	Unit trying to lock onto downstream carrier
Network	Solid Yellow	Unit has locked onto downstream carrier
Network	Periodic Flash Green	Attempted acquiring via OOB SWEEP command
Network	Solid Green	Successful acquisition of the network
Test	Solid Green	Unit has loaded FIPS options and is not in the Error state
Test and Network	Flashing Yellow	Unit has a failure of the FPGAs
Test	Solid Yellow	Unit is in the Error state

Table 2 – Front Panel LEDs

LED	Status Indication	Status Description
All	All lit	Unit's bootloader is starting
Net	Solid Green	Unit's DRAM Test 25% completed
Status	Solid Green	Unit's DRAM test 50% completed
TX	Solid Green	Unit's DRAM test 75% completed
RX	Solid Green	Unit's DRAM test 100% completed
Status	Solid Red	Unit's DRAM test failed.
Status	Solid Green	Unit's DRAM test passed.
Status	Solid Red	Unit's application fails to load.
Status	Solid Green	Unit's application successfully loaded.
Status	Solid Red	Unit has a failure of the FPGAs
10/100 LAN Yellow	N/A	Not Used
10/100 LAN Green	Blinking Green	Traffic over network link.
10/100 LAN Green	Solid Green	Network link detected.
Console Yellow	N/A.	Not Used
Console Green	N/A.	Not Used
RX	Solid Yellow	TDMA remote – SCPC unlocked.
RX	Solid Yellow	TDMA remote OOB – no TDM lock.
RX	Solid Green	TDMA remote – SCPC locked.
RX	Solid Green	TDMA remote OOB – in acquisition.
RX	Solid Green	TDMA remote OOB – in network.
RX	Solid Green	TDMA remote OOB – TX muted
RX	Solid Green	TDMA remote OOB – TDM lock only.
RX	Solid Yellow	iSCPC – demod unlocked
RX	Solid Green	iSCPC – demod locked
TX	Solid Green	TDMA remote OOB – in acquisition.
TX	Solid Green	TDMA remote OOB – in network.
TX	Solid Green	iSCPC – demod unlocked

LED	Status Indication	Status Description
TX	Solid Green	iSCPC – demod locked
Net	Flashing Yellow	TDMA remote – SCPC unlocked.
Net	Flashing Yellow	TDMA remote OOB – no TDM lock.
Net	Solid Yellow	TDMA remote – SCPC locked.
Net	Flashing Green	TDMA remote OOB – in acquisition.
Net	Solid Green	TDMA remote OOB – in network.
Net	Solid Yellow	TDMA remote OOB – TX muted
Net	Solid Yellow	TDMA remote OOB – TDM lock only.
Net	Solid Yellow	iSCPC – demod unlocked
Net	Solid Green	iSCPC – demod locked

Table 3 – Rear Panel LEDs

All of these physical ports are mapped to FIPS 140-2 logical interfaces, as described in the following table:

Module Physical Port	FIPS 140-2 Logical Interface
Power connector	Power interface
Ethernet port	Control input, status output, data input, data output
RX coaxial connector	Control input, data input
TX coaxial connector	Status output, data output
Console port	Control input, status output
Indicators	Status output
Power Button	Control input

Table 4 – Physical Ports and Logical Interfaces

Roles and Services

There are five roles in the module that operators may assume: a Crypto-Officer role, a Bootloader User role, a User role, a Client Crypto-Officer role, and a Client User role.

The Crypto-Officer role has access to the security-relevant configuration and management of the module through a locally accessible CLI. The Bootloader User role has access to a subset of the commands of the User role. The User role has access to non-security-relevant configuration of the module, updating the module's firmware, and monitoring of the module through a network accessible API and CLI. The Client User role accesses the module's link encryption services, and the Client Crypto-Officer role is responsible for configuration of dynamic keys for link encryption.

The Crypto-Officer, Bootloader User, and User roles are authenticated using passwords. However, authentication mechanisms are not tested as part of the FIPS 140-2 Level 1 validation.

Crypto-Officer Role

The Crypto-Officer accesses the module over the console port using a CLI. Through this local access, the Crypto-Officer can manually enter static link encryption keys and passwords, and display configured keys and passwords. Additionally, the Crypto-Officer has access to all of the CLI commands provided to the User role.

The Crypto-Officer role is assumed by authenticating to the "crypto" account using a password. Once authenticated, the Crypto-Officer has access to the services listed in the following table:

Service	Description	Input	Output	Key/CSP	Key/CSP Access
Login	Authenticate the Crypto-Officer role	Login information	Status of login attempt	Crypto-Officer password	Read
$	Processes GPS NMEA message	Command	Command response	None	None
arp	ARP control	Command and sub-command (and configuration information if applicable)	Command response (and statistics if applicable)	None	None
btp stats	Show Burst Timeplan Stats	Command	Command response and statistics	None	None
cpu	CPU performance monitoring and related commands	Command and sub-command	Command response and status information	None	None
csp	Read/write/modify/delete critical security parameters, including (static) Triple-DES keys and the Crypto-Officer password	Command and sub-command (and configuration information, including manually entered keys, if modifying)	Command response (and configuration information, including keys, if reading)	Crypto-Officer password and (static) Triple-DES keys	Read/Write
delay	Sleep	Command	Command response	None	None
demand	Demand control	Command and sub-command (and configuration information if applicable)	Command response (and statistics if applicable)	None	None
dhcp	DHCP server control	Command and sub-command (and configuration information if applicable)	Command response (and statistics if applicable)	None	None
dma	DMA control	Command	Command response	None	None
dns	DNS control	Command and sub-command	Command response (and parameters if applicable)	None	None
dqt	Show/set DQT level	Command and sub-command (and level, if setting)	Command response	None	None
enc	Remote encryption control	Command and sub-command (and configuration information, including manually entered keys, if modifying)	Command response (and configuration information, including keys, if reading)	(Static) Triple-DES keys	Read/Write
encs	Remote encryption session control	Command and sub-command (and configuration information, including manually entered keys, if modifying)	Command response (and configuration information, including keys, if reading)	(Static) Triple-DES keys	Read/Write
errorstate	Manually enter error state	Command	Command response	None	None

Service	Description	Input	Output	Key/CSP	Key/CSP Access
eth	Ethernet Control	Command and sub-command (and enable/disable parameters as needed)	Command response (and statistics if applicable)	None	None
exit	Log out of CLI	Command	Command response	None	None
extras	Read/write/modify extras	Command and sub-command (and configuration information, if modifying)	Command response (and configuration information if reading)	None	None
flash	Flash control	Command and sub-command	Command response (and statistics if applicable)	None	None
heap	Displays and reset heap statistics	Command and sub-command	Command response (and statistics requested if displaying)	None	None
help	Display commands	Command and parameters for specific help items	Command response and help information	None	None
igmp	Multicast control	Command and sub-command	Command response (and statistics if applicable)	None	None
inroute_list	Show Inroute List	Command	Command response and list	None	None
install	Install utility – used to set various options mainly involving network configurations	Command,sub-command, and configuration information	Command response	None	None
ip	Router control	Command and sub-command (and configuration information if applicable)	Command response (and statistics if applicable)	None	None
ipv4	IPv4 control	Command and sub-command (and configuration information if applicable)	Command response (and statistics if applicable)	None	None
key net	View/import network encryption key	Command (and key if importing)	Command response and key	(Static) Triple-DES keys	Read/Write
key rmt	View/import remote encryption key	Command (and key if importing)	Command response and key	(Static) Triple-DES keys	Read/Write
keygen	Generate a Triple-DES key	Command	Command response and Triple-DES key	(Generic) Triple-DES keys	Read/Write
laninfo	Read/write LAN configuration information	Command (and LAN configuration if writing)	Command response and LAN configuration	None	None

Service	Description	Input	Output	Key/CSP	Key/CSP Access
ll	Link Layer control	Command and sub-command (and configuration information if applicable)	Command response (and statistics if applicable)	None	None
load	Load a firmware update	Command and options	Command response	Integrity check RSA public key	Read
mac	MAC control	Command and sub-command	Command response (and statistics if applicable)	None	None
mcvlan	MC-VLAN Layer Control	Command and sub-command (and configuration information if applicable)	Command response (and statistics if applicable)	None	None
nat	NAT control	Command and sub-command	Command response (and statistics if applicable)	None	None
nenc	Network encryption control	Command and sub-command (and configuration information, including manually entered keys, if modifying)	Command response (and configuration information, including keys, if reading)	(Static) Triple-DES keys	Read/Write
nencs	Network encryption session control	Command and sub-command (and configuration information, including manually entered keys, if modifying)	Command response (and configuration information, including keys, if reading)	(Static) Triple-DES keys	Read/Write
offline	Sends the module offline	Command	Command response	None	None
online	Sends the module online	Command	Command response	None	None
oob	OOB control	Command and sub-command	Command response (and statistics if applicable)	None	None
oobc	OOBC control	Command and sub-command	Command response (and statistics if applicable)	None	None
options	Read/write/modify options	Command and sub-command (and configuration information, if modifying)	Command response (and configuration information if reading)	None	None
pad	PAD control	Command and sub-command (and configuration information if applicable)	Command response (and statistics if applicable)	None	None
passwd	Change password	Command and password information	Command response	Crypto-Officer and User passwords	Read/Write
phy	Read PHY status register	Command	Command response	None	None
ping	Ping utility	Command and IP address	Command response and ping output	None	None

Service	Description	Input	Output	Key/CSP	Key/CSP Access
pool	MssgPool Control	Command and sub-command (and configuration information if applicable)	Command response (and statistics if applicable)	None	None
ps	Lists Threads	Command	Command response and thread information	None	None
qos	QoS control	Command and sub-command (and configuration information if applicable)	Command response (and statistics if applicable)	None	None
quit	Log out of CLI	Command	Command response	None	None
remotestate	Displays the Current Remote State	Command	Command response	None	None
reset	Resets the board	Command	Command response	None	None
rmtstat	Toggles printing Remote Status messages	Command	Command response	None	None
rx	RX Control	Command and sub-command (and parameters as needed)	Command response (and statistics requested if applicable)	None	None
sar	SAR control	Command and sub-command (and configuration information if applicable)	Command response (and statistics if applicable)	None	None
scc	SCC control	Command and sub-command	Command response (and statistics requested if displaying)	None	None
scpc	Display/Reset SCPC statistics	Command	Command response (and statistics requested if displaying)	None	None
sig	Display/verify signatures in flash	Command and sub-command	Command response (and signatures list if applicable)	Integrity check RSA public key	Read
sn	Read/write the board serial number	Command (and serial number if writing)	Command response and serial number	None	None
sockets	Displays socket status	Command	Command response and socket status	None	None
spoof	TCP acceleration control	Command and sub-command (and configuration information if applicable)	Command response (and statistics if applicable)	None	None
status	Display module's status	Command	Command response	None	None
sweeplog	Toggles Sweep Log info	Command	Command response	None	None

Service	Description	Input	Output	Key/CSP	Key/CSP Access
tdma	Display/Reset TDMA statistics	Command	Command response (and statistics requested if displaying)	None	None
timer	Timer control	Command and sub-command	Command response (and statistics if applicable)	None	None
toggleucp	Toggles Printing UCP Command Received	Command	Command response	None	None
tx	TX Control	Command and sub-command (and parameters as needed)	Command response (and statistics requested if applicable)	None	None
uart	Prints stats for uart	Command and sub-command	Command response (and statistics if applicable)	None	None
ucplog	Toggles Printing Transmitter Adjustments and DMATrailer	Command	Command response	None	None
udp	UDP control	Command and sub-command (and configuration information if applicable)	Command response (and statistics if applicable)	None	None
version	Display build information	Command	Command response and version information	None	None
vlan	Vlan control	Command and sub-command (and configuration information if applicable)	Command response (and statistics if applicable)	None	None
xoff	Disallow messages from other processes	Command	Command response	None	None
xon	Allow messages from other processes	Command	Command response	None	None
zeroize	Zeroize all critical security parameters at a global level, network level, or remote level	Command	Command response	All	Write

Table 5 – Crypto-Officer Services

Bootloader User Role

The Bootloader User accesses the module over the console port using a CLI. The Bootloader User is primarily used for debugging the module, using a subset of the CLI commands available to the User role, including the ability to manually update the module's firmware.

The Bootloader User role is assumed by entering into the bootloader console CLI during boot up of the module and authenticating to the bootloader "admin" account with the default password. This password cannot be changed, and for FIPS purposes, the role is considered unauthenticated. The Bootloader User has access to the services listed in the following table:

Service	Description	Input	Output	Key/CSP	Key/CSP Access
arp	ARP control	Command and sub-command (and configuration information if applicable)	Command response (and statistics if applicable)	None	None
errorstate	Manually enter bootloader error state	Command	Command response	None	None
cpu	CPU performance monitoring and related commands	Command and sub-command	Command response and status information	None	None
delay	Sleep	Command	Command response	None	None
eth	Ethernet Control	Command and sub-command (and enable/disable parameters as needed)	Command response (and statistics if applicable)	None	None
exit	Log out of CLI	Command	Command response	None	None
flash	Flash control	Command and sub-command	Command response (and statistics if applicable)	None	None
help	Display commands	Command and parameters for specific help items	Command response and help information	None	None
igmp	Multicast control	Command and sub-command	Command response (and statistics if applicable)	None	None
ip	Router control	Command and sub-command (and configuration information if applicable)	Command response (and statistics if applicable)	None	None
laninfo	Read/write LAN configuration information	Command (and LAN configuration if writing)	Command response and LAN configuration	None	None
load	Load a firmware update	Command and options, including HMAC key	Command response	HMAC firmware update key	Write
mac	MAC control	Command and sub-command	Command response (and statistics if applicable)	None	None
options	Read/write/modify options	Command and sub-command (and configuration information)	Command response (and configuration information if reading)	None	None

Service	Description	Input	Output	Key/CSP	Key/CSP Access
pool	MssgPool Control	Command and sub-command (and configuration information if applicable)	Command response (and statistics if applicable)	None	None
ps	Lists Threads	Command	Command response and thread information	None	None
quit	Log out of CLI	Command	Command response	None	None
reset	Resets the board	Command	Command response	None	None
sn	Read/write the board serial number	Command (and serial number if writing)	Command response and serial number	None	None
status	Display module's status	Command	Command response	None	None
timer	Timer control	Command and sub-command	Command response (and statistics if applicable)	None	None
toggleucp	Toggles Printing UCP Command Received	Command	Command response	None	None
uart	Prints stats for uart	Command and sub-command	Command response (and statistics if applicable)	None	None
version	Display build information	Command	Command response and version information	None	None
xoff	Disallow messages from other processes	Command	Command response	None	None
xon	Allow messages from other processes	Command	Command response	None	None
zeroize	Zeroize all critical security parameters at a global level, network level, or remote level	Command	Command response	All	Write

Table 6 – Bootloader User Services

User Role

The User accesses the module over the RX/TX/Ethernet ports through an API or CLI and over the console port using a CLI. The User can perform non-security-relevant configuration and monitoring of the module. Additionally, the User role is able to update the module's firmware using the multicast firmware update provided through the API or the "load" command provided through the CLI. The User's access to the module over the RX/TX ports also utilizes the module's traffic routing and link encryption services (see Client User role).

The User role is assumed by authenticating to the "admin", "diagnostic", or "user" accounts using a password. The User has access to the services listed in the following table:

Service	Description	Input	Output	Key/CSP	Key/CSP Access
Antenna alignment configuration	Change the pointing mode or continuous wave mode for the antenna	Command and the option to enable or disable the mode	Command response	None	None
Enabling/disabling RX and TX	Enable or disable the RX and TX ports	Command and option to enable or disable the RX and TX	Command response	None	None
Link Layer Monitoring	Start and stop output of link layer messages for debugging from the module	Command to start or stop link layer messages and proper parameters	Command response	None	None
Option file uploading and downloading	Send to the module or receive from the module configuration information (i.e., an options file)	Command (and options file for download)	Command response (and options file for upload)	None	None
Package downloading	Send to the module a package containing firmware	Command and package	Command response	None	None
Reset the module	Resets the module (i.e., the module restarts)	Command	None	None	None
Set modem parameters	Configures internal parameters of the module	Command and parameter	Command response	None	None
Setting geographic location	Sets geographic location Latitude and Longitude parameters	Command and parameters	Command Response	None	None
Setting modem offline	Disables the module	Command	Command response	None	None
Setting notification status	Enables or disables the notifications sent out by the module	Command and enable or disable option	Command response	None	None
TX configuration settings	Change the transmit power or frequency	Command and the power or frequency as a parameter	Command response	None	None
Viewing and resetting transmitter and receiver statistics	Retrieve or reset the module's transmitter and receiver statistics	Command	Command (and statistics if viewing)	None	None
Viewing firmware version or board information	Retrieve the firmware version or board information from the module	Command	Command response	None	None

Service	Description	Input	Output	Key/CSP	Key/CSP Access
Viewing or resetting Ethernet statistics	Retrieve or reset the module's Ethernet statistics	Command	Command response (and Ethernet statistics if viewing)	None	None
Viewing RF statistics	Retrieve the RF statistics from the module	Command	Command response and RF statistics	None	None
Login	Authenticate the User role	Login information	Status of login attempt	User passwords	Read
$	Processes GPS NMEA message	Command	Command response	None	None
arp	ARP control	Command and sub-command (and configuration information if applicable)	Command response (and statistics if applicable)	None	None
btp stats	Show Burst Timeplan Stats	Command	Command response and statistics	None	None
cpu	CPU performance monitoring and related commands	Command and sub-command	Command response and status information	None	None
delay	Sleep	Command	Command response	None	None
demand	Demand control	Command and sub-command (and configuration information if applicable)	Command response (and statistics if applicable)	None	None
dhcp	DHCP server control	Command and sub-command (and configuration information if applicable)	Command response (and statistics if applicable)	None	None
dma	DMA control	Command	Command response	None	None
dns	DNS control	Command and sub-command	Command response (and parameters if applicable)	None	None
dqt	Show/set DQT level	Command and sub-command (and level, if setting)	Command response	None	None
dumpb	Dumps bursts received on hub	Command and options	Command response and dumped bursts	None	None
eth	Ethernet Control	Command and sub-command (and enable/disable parameters as needed)	Command response (and statistics if applicable)	None	None
exit	Log out of CLI	Command	Command response	None	None

Service	Description	Input	Output	Key/CSP	Key/CSP Access
extras	Read/write/modify extras	Command and sub-command (and configuration information)	Command response (and configuration information if reading)	None	None
flash	Flash control	Command and sub-command	Command response (and statistics if applicable)	None	None
heap	Displays and reset heap statistics	Command and sub-command	Command response (and statistics requested if displaying)	None	None
help	Display commands	Command and parameters for specific help items	Command response and help information	None	None
igmp	Multicast control	Command and sub-command	Command response (and statistics if applicable)	None	None
inroute_list	Show Inroute List	Command	Command response and list	None	None
ip	Router control	Command and sub-command (and configuration information if applicable)	Command response (and statistics if applicable)	None	None
ipv4	IPv4 control	Command and sub-command (and configuration information if applicable)	Command response (and statistics if applicable)	None	None
laninfo	Read/write LAN configuration information	Command (and LAN configuration if writing)	Command response and LAN configuration	None	None
ll	Link Layer control	Command and sub-command (and configuration information if applicable)	Command response (and statistics if applicable)	None	None
load	Load a firmware update	Command and options	Command response	Integrity check RSA public key	Read
mac	MAC control	Command and sub-command	Command response (and statistics if applicable)	None	None
mcvlan	MC-VLAN Layer Control	Command and sub-command (and configuration information if applicable)	Command response (and statistics if applicable)	None	None
nat	NAT control	Command and sub-command	Command response (and statistics if applicable)	None	None

Service	Description	Input	Output	Key/CSP	Key/CSP Access
offline	Sends the module offline	Command	Command response	None	None
online	Sends the module online	Command	Command response	None	None
oob	OOB control	Command and sub-command	Command response (and statistics if applicable)	None	None
oobc	OOBC control	Command and sub-command	Command response (and statistics if applicable)	None	None
options	Read/write/modify options	Command and sub-command (and configuration information)	Command response (and configuration information if reading)	None	None
pad	PAD control	Command and sub-command (and configuration information if applicable)	Command response (and statistics if applicable)	None	None
passwd	Change password	Command and password information	Command response	User passwords	Read/Write
ping	Ping utility	Command and IP address	Command response and ping output	None	None
pool	MssgPool Control	Command and sub-command (and configuration information if applicable)	Command response (and statistics if applicable)	None	None
ps	Lists Threads	Command	Command response and thread information	None	None
qos	QoS control	Command and sub-command (and configuration information if applicable)	Command response (and statistics if applicable)	None	None
quit	Log out of CLI	Command	Command response	None	None
remotestate	Displays the Current Remote State	Command	Command response	None	None
reset	Resets the board	Command	Command response	None	None
rmtstat	Toggles printing Remote Status messages	Command	Command response	None	None
rx	RX Control	Command and sub-command (and parameters as needed)	Command response (and statistics requested if applicable)	None	None

Service	Description	Input	Output	Key/CSP	Key/CSP Access
sar	SAR control	Command and sub-command (and configuration information if applicable)	Command response (and statistics if applicable)	None	None
scc	SCC control	Command and sub-command	Command response (and statistics requested if displaying)	None	None
scpc	Display/Reset SCPC statistics	Command	Command response (and statistics requested if displaying)	None	None
sig	Display/verify signatures in flash	Command and sub-command	Command response (and signatures list if applicable)	Integrity check RSA public key	Read
sn	Read/write the board serial number	Command (and serial number if writing)	Command response and serial number	None	None
sockets	Displays socket status	Command	Command response and socket status	None	None
spoof	TCP acceleration control	Command and sub-command (and configuration information if applicable)	Command response (and statistics if applicable)	None	None
status	Display module's status	Command	Command response	None	None
sweeplog	Toggles Sweep Log info	Command	Command response	None	None
tdma	Display/Reset TDMA statistics	Command	Command response (and statistics requested if displaying)	None	None
timer	Timer control	Command and sub-command	Command response (and statistics if applicable)	None	None
toggleucp	Toggles Printing UCP Command Received	Command	Command response	None	None
tx	TX Control	Command and sub-command (and parameters as needed)	Command response (and statistics requested if applicable)	None	None
uart	Prints stats for uart	Command and sub-command	Command response (and statistics if applicable)	None	None

Service	Description	Input	Output	Key/CSP	Key/CSP Access
ucplog	Toggles Printing Transmitter Adjustments and DMATrailer	Command	Command response	None	None
udp	UDP control	Command and sub-command (and configuration information if applicable)	Command response (and statistics if applicable)	None	None
version	Display build information	Command	Command response and version information	None	None
vlan	Vlan control	Command and sub-command (and configuration information if applicable)	Command response (and statistics if applicable)	None	None
xoff	Disallow messages from other processes	Command	Command response	None	None
xon	Allow messages from other processes	Command	Command response	None	None
zeroize	Zeroize all critical security parameters at a global level, network level, or remote level	Command	Command response	All	Write

Table 7 – User Services

Client Crypto-Officer Role

The Client Crypto-Officer role accesses the module using the Out Of Band (OOB) messages provided below the iDirect Link Layer (LL) of the module. Besides performing non-security-relevant functions, these commands configure dynamic keys for link encryption. The Client Crypto-Officer role is implicitly assumed by an entity utilizing the OOB messages – either another NetModem or the Protocol Processor.

The Client Crypto-Officer role services are listed in the following table:

Service	Description	Input	Output	Key/CSP	Key/CSP Access
Link Encryption Initialization and Configuration OOB Messages	These link layer messages initialize and configure link encryption	OOB message inputs, including keys, and control	OOB message outputs, including keys, and status	(Dynamic) Triple-DES session keys Key transport RSA public key	Read/write Write
General Out Of Band (OOB) Messages	These link layer messages perform low-level configuration and monitoring of the module (all non-security-relevant)	OOB message inputs and control	OOB message outputs and status	None	None

Table 8 – Client Crypto-Officer Services

Client User Role

The Client User role accesses the module over the Ethernet and RX/TX 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.

The Client User role services are listed in the following table:

Service	Description	Input	Output	Key/CSP	Key/CSP Access
Link Encryption and Traffic Routing	The modules bulk data encryption/decryption at the data-link layer	Link layer encryption inputs and data	Link layer encryption output and data	(Static or dynamic) Triple-DES session keys	Read

Table 9 – Client User Services

Physical Security

The NetModem II Plus is a multi-chip standalone cryptographic module. The module's hardware is composed of production-grade components and is entirely enclosed in a solid metal case. This case encloses all of the module's internal components and serves as the cryptographic boundary for the module.

The NetModem was tested and found conformant to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B (i.e., for home use).

Operational Environment

The operational environment requirements do not apply to the NetModem. The module does not provide a general purpose Operating System (OS) and only allows the updating of its firmware components using RSA digitally signed or SHA-1 HMAC'd firmware updates.

Cryptographic Key Management

The NetModem II Plus implements the following FIPS-approved algorithms:

- RSA (implemented in software with modular exponentiation performed in hardware) – PKCS#1 (vendor affirmed)
- SHA-1 (implemented in software) – FIPS 180-2 (certificate 220)
- HMAC SHA-1 (implemented in software) – FIPS 198 (vendor affirmed, SHA-1 certificate 220)
- Deterministic Random Number Generator (RNG) (implemented in software) – Appendix A.2.4 of ANSI X9.31
- Triple-DES CBC mode (implemented in hardware) – FIPS 46-3 (certificate 242)

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

- HiFn 7902 Hardware RNG – for seeding the X9.31 RNG

The NetModem II Plus supports the following keys and CSPs:

Key or CSP	Key type	Generation	Storage	Use
Dynamic Triple-DES link encryption keys	Triple-DES (168 bits)	Either internally generated (random data from the module's X9.31 RNG), or externally generated and loaded onto the module by the Client Crypto-Officer (rekeying over a Triple-DES encrypted link)	Volatile memory (plaintext)	Link encryption
Static Triple-DES link encryption keys	Triple-DES (168 bits)	Externally generated and manually entered by the Crypto-Officer (over the directly connected console port)	Non-volatile memory (flash - plaintext)	Link encryption
Generic Triple-DES keys	Triple-DES (168 bits)	Internally generated and output by the Crypto-Officer (over the directly connected console port)	Volatile memory (plaintext)	Generic Triple-DES keys for use as required
Firmware update HMAC key	HMAC (160 bits)	Externally generated and loaded onto the module by the Crypto-Officer (over the directly connected console port)	Volatile memory (plaintext)	Firmware update test (HMAC verification)
Crypto-Officer role password	CSP	N/A	Non-volatile memory (flash - plaintext)	Authenticate the Crypto-Officer role
User role passwords	CSP	N/A	Non-volatile memory (flash - plaintext)	Authenticate the User role
X9.31 RNG seed and seed keys	Triple-DES (112 bits)	Internally generated by the Hardware RNG (not used for data encryption)	Volatile memory (plaintext)	Used by X9.31 RNG
Integrity check RSA public key	RSA (2048 bits)	Externally generated and hard-coded into the module's firmware	Non-volatile memory (flash - plaintext)	Firmware integrity check and multicast firmware update
Key transport RSA public key	RSA (2048 bits)	Externally generated and entered by the Client Crypto-Officer	Volatile memory (plaintext)	Key transport

Table 10 – Listing of Keys and CSPs

Triple-DES link encryption secret keys encrypt/decrypt Client User data traffic flowing between the NetModem and the iDirect Protocol Processor or another NetModem. These keys can either be statically configured or dynamically generated. When dynamically generated, the initial link encryption key is generated internally by the module and subsequent dynamic keys (i.e., for re-keying) are loaded onto the module by the Client Crypto-Officer (Triple-DES encrypted). When statically configured, the keys are externally generated and manually entered by the Crypto-Officer (over the directly connected console port). Dynamically configured keys are stored in volatile memory, and statically configured keys are stored in non-volatile memory (flash).

Generic Triple-DES keys are not used internally by the module and are output from the module for general use by the Crypto-Officer. The keys are internally generated by the module using a CLI command and are

immediately output from the module after generation in plaintext over the directly connected console port. These keys are stored in volatile memory only.

Firmware update HMAC keys verify the HMAC on a firmware update. These keys are externally generated and loaded onto the module by the Bootloader User (over the directly connected console port) during the firmware update process. These keys are stored in volatile memory only.

The Crypto-Officer and User passwords are configured by their respective roles or by the Crypto-Officer role. These passwords authenticate the Crypto-Officer or User roles, and are stored in non-volatile memory (flash).

The X9.31 deterministic RNG seed and seed keys are generated by taking random data from the internal hardware RNG. These values are stored in volatile memory.

The integrity check RSA public key is hard-coded into the module's firmware. This key is externally generated and verifies the integrity of the module's firmware image during power-up and for verifying the signatures calculated over multicast firmware updates. This key is stored in non-volatile memory (flash).

The key transport RSA public key is loaded onto the module by the Client Crypto-Officer. This key is externally generated and is used for key transport during dynamic keying for link encryption. This key is stored in volatile memory.

All volatile and non-volatile secret keys and CSPs (passwords, seeds, etc.) on the module can be zeroized using the module's global zeroize command. The module must be reconfigured after this command is issued.

Self-Tests

The NetModem performs the following self-tests at power-up:

- Firmware integrity check – SHA-1 check over the bootloader and RSA digital signature over all of the module's firmware (including the bootloader).
- Known Answer Tests (KATs)
    - Triple-DES
    - SHA-1

- SHA-1 HMAC
- X9.31 RNG

The NetModem performs the following conditional self-tests:

- Continuous RNG tests for the X9.31 RNG and the hardware RNG (HiFn 7902) whenever the RNG's generate random data.
- Manual key entry test whenever Triple-DES or SHA-1 HMAC keys are manually entered into the module. An error detection code (EDC) is verified over the key, and the key is rejected if verification fails.
- Multicast firmware update test whenever a multicast firmware update is received by the module. An RSA digital signature is verified over the update, and the update is rejected if verification fails.
- Firmware update test whenever a firmware update is received by the module. An HMAC is verified over the update, and the update is rejected if verification fails.

If the power-up self-tests or the continuous RNG tests fail, the module enters the error state, displays status output, inhibits data output, and halts cryptographic operations. If the power-up self-tests pass, the module outputs a status message and continues on with its startup. If the manual key entry test or firmware update tests fail, the module will reject the requested service, and display status output.

Design Assurance

iDirect uses the Concurrent Versions System (CVS) to perform configuration management for the module's source code, hardware design information, and other components. iDirect also has a formal process governing releases and utilizes Bugzilla for change request tracking.

Additionally, Microsoft Visual Source Safe (VSS) version 6.0 is used to provide configuration management for the module's FIPS documentation. This software provides access control, versioning, and logging.

Mitigation of Other Attacks

This section is not applicable. The NetModem does not employ security mechanisms to mitigate specific attacks.

SECURE OPERATION

The NetModem II Plus is FIPS-compliant by default and meets Level 1 requirements for FIPS 140-2 without any special configuration instructions.

Crypto-Officer Guidance

The Crypto-Officer is responsible for initialization, and security-relevant configuration and management of the module through the console port. Please see iDirect's *Crypto-Officer Manual* for more information on configuring and maintaining the module.

Initialization

When the module is initially received by the Crypto-Officer, a default Crypto Officer password is configured. The module will remain in an Error state (limited status commands available only) until the Crypto Officer logs in and changes the password.

After changing the default Crypto-Officer password, the Crypto-Officer is ready to configure and manage the module.

Management

The Crypto-Officer can configure the module's security-relevant settings, including manual entry of static Triple-DES session keys and account passwords.

The Crypto-Officer should routinely check the NetModem's logs and other status information to ensure the module is functioning properly. If the NetModem consistently malfunctions or otherwise repeatedly enters an error state, iDirect should be contacted.

Zeroization

The Crypto-Officer has access to a global zeroization command that zeroizes all of the module's secret keys and CSPs.

Bootloader User Guidance

The Bootloader User is responsible for debugging and recovery of the module if difficulties arise in the primary application. This role accesses the module before the primary application is executed through a CLI provided by the bootloader console.

Management

The Bootloader User should only access the module for debugging or recovery purposes. This role has access to a limited view of the module through a subset of the CLI commands provided to the User.

Additionally, the Bootloader User can load HMAC'd firmware updates onto the module, and as part of this update, must manually enter a HMAC key. The Bootloader User must ensure that the updates being loaded are FIPS-validated, and updating of the module's firmware by the Bootloader User should only be performed to recover the module.

User Guidance

The User is responsible for non-security-relevant management of the module and updating of the module's firmware through the RX/TX/Ethernet ports.

Management

The User can manage the module's non-security settings and monitor the module's status. These capabilities include configuration of various satellite communications options, quality of service settings, and other functionality (as detailed in Table 7 above).

Additionally, the User can load RSA digitally signed firmware updates onto the module, and the User must ensure that the updates being loaded are FIPS-validated. This loading of firmware updates can occur through commands provided by the CLI or through calls to the API.

The User should routinely check the NetModem's logs and other status information to ensure the module is functioning properly. If the NetModem consistently malfunctions or otherwise repeatedly enters an error state, the User should notify the Crypto-Officer immediately.

Client Crypto-Officer Guidance

The Client Crypto-Officer configures the module's dynamic link encryption keys through OOB messages. Dynamic Triple-DES session keys must be entered into or output from the module in an encrypted form, and the module enforces this restriction by default.

Client User Guidance

The Client User accesses the module's link encryption services as configured by the Crypto-Officer. There are no special instructions for the Client User to take to use the module securely.

ACRONYMS

ANSI	American National Standards Institute
API	Application Programming Interface
ARP	Address Resolution Protocol
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CPU	Central Processing Unit
CSP	Critical Security Parameter
CVS	Concurrent Versions System
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
DRAM	Dynamic Random Access Memory
DQT	Digital Quadrature Tuner
EDC	Error Detection Code
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
FPGA	Field Programmable Gate Array
GPS	Global Positioning System
HMAC	(Keyed-) Hash Message Authentication Code
IF	Interface
IP	Internet Protocol
KAT	Known Answer Test
LAN	Local Area Network
LED	Light Emitting Diode
MAC	Machine Address Code
MC-VLAN	Multicast Virtual Local Area Network
NAT	Network Address Translation
NIST	National Institute of Standards and Technology
NMEA	National Marine Electronics Association
OOB	Out Of Band
OOBC	Out Of Band Chunk
OS	Operating System
PAD	Packet Assembler / Disassembler
PHY	Physical Layer
PKCS	Public Key Cryptography Standards
QoS	Quality of Service
RAM	Random Access Memory
RNG	Random Number Generator
RSA	Rivest Shamir and Adleman
RX	Receive
SAR	Segmentation And Reassembly
SCC	Switching Control Center
SCPC	Single Channel Per Carrier
SHA	Secure Hash Algorithm

TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TDMA	Time Division Multiple Access
TX	Transmit
UCP	Uplink Control Process
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VSAT	Very Small Aperture Terminal
VSS	Visual Source Safe

