Protocol Processor v5.0

(Hardware Version 5.0,
Software 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 a non-proprietary Cryptographic Module Security Policy for the Protocol Processor v5.0 from iDirect Technologies (iDirect). This security policy describes how the Protocol Processor v5.0 meets the security requirements of FIPS 140-2 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 (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 Protocol Processor v5.0 is referred to in this document as the Protocol Processor 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.

PROTOCOL PROCESSOR

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 Protocol Processor is a multi-chip standalone cryptographic module that meets overall FIPS 140-2 Level 1 requirements. The module is constructed from a production-grade rack-mountable IBM xSeries 335 server running the general purpose Operating System (OS) RedHat Linux version 7.3 with custom iDirect software installed. The cryptographic boundary of the Protocol Processor is the metal case of the xSeries 335 server.

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	EMI/EMC	1
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 Protocol Processor is built from the IBM xSeries 335 rack-mountable server and includes the following physical ports (not all listed physical ports are utilized by the iDirect software),

- Diskette drive (1.44MB) and diskette-eject button (not used by the iDirect software)
- CD-ROM drive and CD-ROM drive-eject button (not used by the iDirect software)
- Power connector
- Two Cable Chaining Technology (C2T) ports (one IN, one OUT)
- One ISM connector (not used by the iDirect software)
- Two 10/100/1000 Ethernet ports
- Three Universal Serial Bus (USB) connectors
- One Serial port
- Multiple Light Emitting Diodes (LEDs)
- Power control button
- Select button
- Reset button

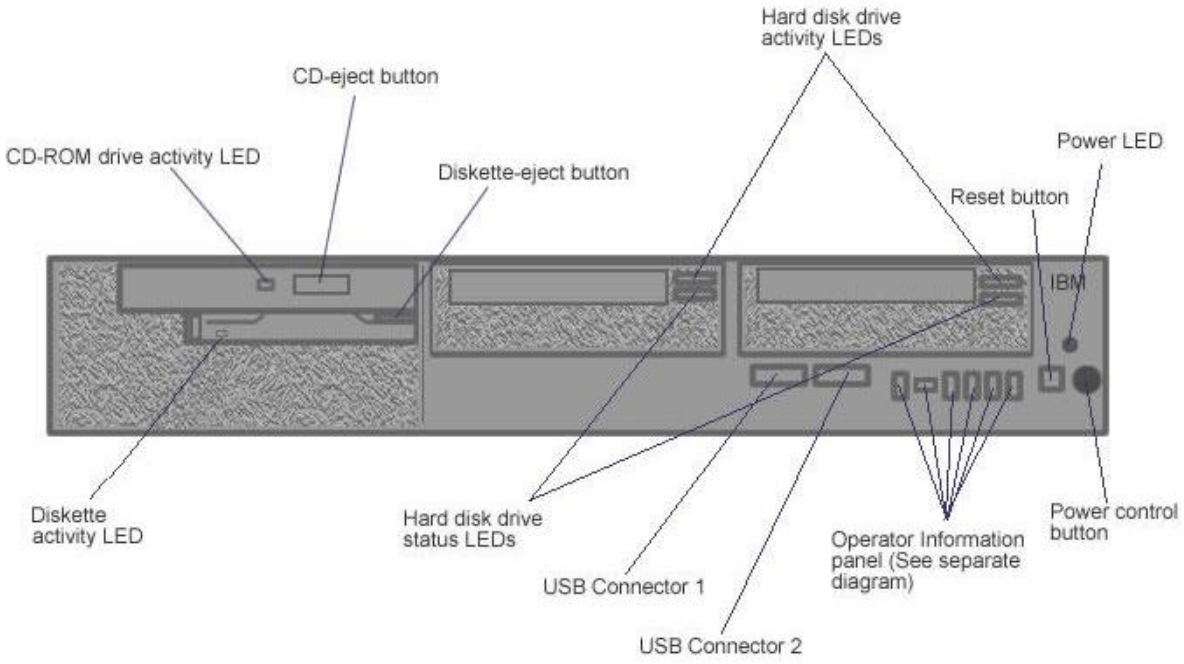

Figure 1 – Front Panel Physical Ports

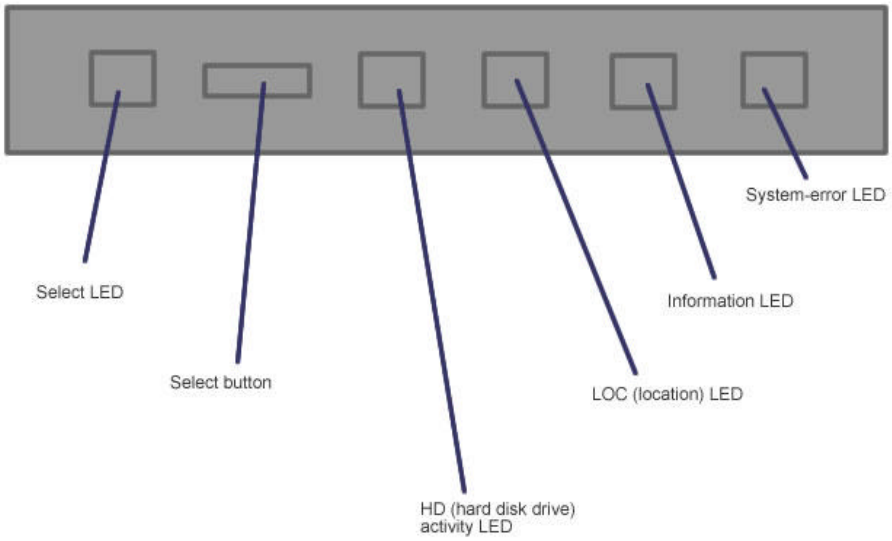

Figure 2 – Operator Information Panel

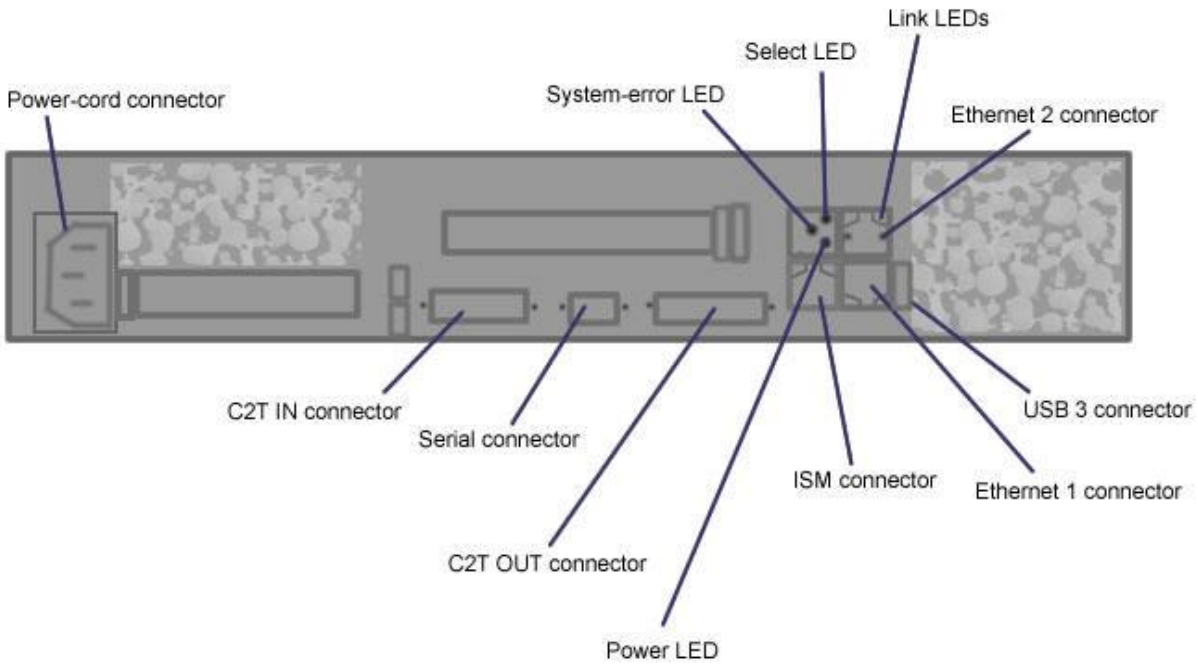

Figure 3 – Rear Panel Physical Ports

The LEDs provide status indication for the Protocol Processor, as detailed in the following table.

LED	Status Indication	Status Description
Diskette drive activity LED	Lit	Diskette drive activity is occurring.
CD-ROM drive activity LED	Lit	CD-ROM drive activity is occurring.
Hard disk drive activity LEDs	Lit	Hard drive activity is occurring.
Hard disk drive status LEDs	Lit	Hard drive failure.
Power LED	Lit solid	Power is connected, and the server is turned on.
Power LED	Flashing	Power is connected, and the server is in standby.
System-error LED	Lit	System error occurred (hardware).
Information LED	Lit	Non-critical event occurred.
LOC (location) LED	Lit	Locator LED blinks when requested to indicate the location of the server.
HD (hard disk drive) activity LED	Lit	Hard drive activity is occurring.
Select LED	Lit	The server is using the monitor, keyboard, and mouse connected to the C2T chain.

Table 2 – Front Panel LEDs

LED	Status Indication	Status Description
Power LED	Lit solid	Power is connected and the server is turned on.
Power LED	Flashing	Power is connected and the server is in standby.
System-error LED	Lit	System error occurred (hardware).
Select LED	Lit	The server is using the monitor, keyboard, and mouse connected to the C2T chain.
Link LEDs	Lit	Network link detected.

Table 3 – Rear Panel LEDs

The Protocol Processor consists of a rack-mount server running a general purpose OS with custom iDirect software. All of the module's physical ports are mapped to the FIPS 140-2 logical interfaces as described in the following table.

Protocol Processor Physical Port	FIPS 140-2 Logical Interface
Power connector	Power interface
Ethernet ports	Control input, status output, data input, data output
Serial port ("console" port)	Control input, status output
C2T OUT port ("console" port)	Control input, status output
USB ports ("console" port)	Control input
ISM port	Not used by module's software
Diskette drive	Not used by module's software
CDROM drive	Not used by module's software
Indicators	Status output
Select Button	Control input
Reset Button	Control input
Power Button	Control input
C2T IN port	None (pass-through control of a IBM xSeries 335 series server)

Table 4 – Physical Ports and Logical Interfaces

The Protocol Processor's software is composed of four primary components: a daemon to provide the module's services, a driver to interface with the module's cryptographic chip, a script to start and stop the daemon, and a second script to ensure the module's daemon is running. These components make up the iDirect module's software running on the Linux OS.

Roles and Services

There are four roles in the module that operators may assume: a Crypto-Officer 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 User role has access to non-security-relevant configuration 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 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 locally over the console ports 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
arp	ARP control	Command and sub-command (and configuration information if applicable)	Command response (and statistics if applicable)	None	None
clear	Clear console screen	Command	Command response	None	None
csp	Read/write/modify/delete critical security parameters, including (static) Triple-DES keys and the Crypto-Officer password, for the global configuration, network configuration, and remote configuration	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
da	DA control	Command and sub-command (and configuration information if applicable)	Command response (and statistics if applicable)	None	None
debug	Network outroute debug control	Command and level	Command response	None	None
downrt	Downrt stats	Command and sub-command (and options if applicable)	Command response (and statistics if applicable)	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
exit	Log out of CLI	Command	Command response	None	None
gecho	Global echo	Command and string	Command response and string	None	None
help	Display global level 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

Service	Description	Input	Output	Key/CSP	Key/CSP Access
ip	Router control	Command and sub-command (and configuration information if applicable)	Command response (and statistics if applicable)	None	None
ipstats	IP stats	Command and sub-command (and options if applicable)	Command response (and statistics if applicable)	None	None
ipv4	IPv4 control	Command and sub-command (and options if applicable)	Command response (and statistics if applicable)	None	None
keygen	Generate a Triple-DES key	Command	Command response and Triple-DES key	(Generic) Triple-DES keys	Read/Write
ll	Link Layer control	Command and sub-command (and options if applicable)	Command response (and statistics if applicable)	None	None
mac	MAC control	Command and sub-command	Command response (and statistics if applicable)	None	None
mcvlan	Network VLAN control	Command and sub-command (and options if applicable)	Command response (and statistics if applicable)	None	None
mem	Resource information	Command	Command response	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
net	Network level handling, including viewing/importing of static keys	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
oobc	OOBC control	Command and sub-command	Command response (and statistics if applicable)	None	None
pad	PAD control	Command and sub-command (and options if applicable)	Command response (and statistics if applicable)	None	None
params	Show global level params	Command	Command response	None	None
params (or net-params)	Network params	Command and sub-command (and options if applicable)	Command response (and statistics if applicable)	None	None

Service	Description	Input	Output	Key/CSP	Key/CSP Access
passwd	Change password	Command and password information	Command response	Crypto-Officer and User passwords	Read/Write
proxy	Multicast proxy	Command and sub-command (and configuration information if applicable)	Command response (and statistics if applicable)	None	None
ps	Packet socket	Command and sub-command (and options if applicable)	Command response (and statistics if applicable)	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
reset	Reset global, network, or remote	Command	Command response	None	None
rh	Remote handler control	Command and sub-command (and options if applicable)	Command response (and statistics if applicable)	None	None
rmt	Remote level handling	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
sar	SAR control	Command and sub-command (and options if applicable)	Command response (and statistics if applicable)	None	None
satdbg	Satellite tracking debug control	Command and enable/disable parameter	Command response	None	None
spoof	TCP acceleration control	Command and sub-command (and options if applicable)	Command response (and statistics if applicable)	None	None
stack	Protocol stack control	Command and sub-command (and options if applicable)	Command response (and statistics if applicable)	None	None
stats	Show global level stats	Command	Command response	None	None
stats (or net-stats)	Network stats	Command	Command response	None	None
status	System status report	Command	Command response	None	None
status	Network status report	Command	Command response	None	None
status	Remote or network status report	Command	Command response	None	None

Service	Description	Input	Output	Key/CSP	Key/CSP Access
TERMINATE	Kill process	Command and process	Command response	None	None
timer	Timer control	Command	Command response	None	None
tlev	Trace control	Command (and level if applicable)	Command response (and level if applicable)	None	None
tpdump	Dump timeplan	Command and enable/disable parameter	Command response	None	None
tunnel	Tunnel control	Command and sub-command (and options if applicable)	Command response (and statistics if applicable)	None	None
txodu	Remote ODU control	Command	Command response	None	None
txpower	Set remote tx power	Command and options	Command response	None	None
udp	UDP control	Command and sub-command (and options if applicable)	Command response (and statistics if applicable)	None	None
version	Display build information	Command	Command response and version information	None	None
vlan	Remote VLAN control	Command and sub-command (and options if applicable)	Command response (and statistics if applicable)	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

User Role

The User accesses the module over an Ethernet port through an API or CLI and over the console ports using a CLI. The User can perform non-security-relevant configuration and monitoring of the module. The User's access to the module over the Ethernet port may also utilize 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
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
Options configuration	Send network and remote configuration information to the module	Command and options	Command response	None	None
Query configuration	Retrieve configuration information from the module	Command	Command response and configuration information	None	None
View or reset parameters and statistics	Retrieve various statistics about remotes, reset remotes, reset the remote's link layer, or force re-acquisition of the remote.	Command	Command response (and statistics if applicable)	None	None
Login	Authenticate the User role	Login information	Status of login attempt	User passwords	Read
arp	ARP control	Command and sub-command (and configuration information if applicable)	Command response (and statistics if applicable)	None	None
clear	Clear console screen	Command	Command response	None	None
da	DA control	Command and sub-command (and configuration information if applicable)	Command response (and statistics if applicable)	None	None
debug	Network outroute debug control	Command and level	Command response	None	None
downrt	Downrt stats	Command and sub-command (and options if applicable)	Command response (and statistics if applicable)	None	None
exit	Log out of CLI	Command	Command response	None	None
gecho	Global echo	Command and string	Command response and string	None	None
help	Display global level 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

Service	Description	Input	Output	Key/CSP	Key/CSP Access
ip	Router control	Command and sub-command (and configuration information if applicable)	Command response (and statistics if applicable)	None	None
ipstats	IP stats	Command and sub-command (and options if applicable)	Command response (and statistics if applicable)	None	None
ipv4	IPv4 control	Command and sub-command (and options if applicable)	Command response (and statistics if applicable)	None	None
ll	Link Layer control	Command and sub-command (and options if applicable)	Command response (and statistics if applicable)	None	None
mac	MAC control	Command and sub-command	Command response (and statistics if applicable)	None	None
mcvlan	Network VLAN control	Command and sub-command (and options if applicable)	Command response (and statistics if applicable)	None	None
mem	Resource information	Command	Command response	None	None
net	Network level handling	Command	Command response	None	None
oobc	OOBC control	Command and sub-command	Command response (and statistics if applicable)	None	None
pad	PAD control	Command and sub-command (and options if applicable)	Command response (and statistics if applicable)	None	None
params	Show global level params	Command	Command response	None	None
params (or net-params)	Network params	Command and sub-command (and options if applicable)	Command response (and statistics if applicable)	None	None
passwd	Change password	Command and password information	Command response	User passwords	Read/Write
proxy	Multicast proxy	Command and sub-command (and configuration information if applicable)	Command response (and statistics if applicable)	None	None
ps	Packet socket	Command and sub-command (and options if applicable)	Command response (and statistics if applicable)	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

Service	Description	Input	Output	Key/CSP	Key/CSP Access
reset	Reset global, network, or remote	Command	Command response	None	None
rh	Remote handler control	Command and sub-command (and options if applicable)	Command response (and statistics if applicable)	None	None
rmt	Remote level handling	Command	Command response	None	None
rmt	Remote level handling	Command	Command response	None	None
sar	SAR control	Command and sub-command (and options if applicable)	Command response (and statistics if applicable)	None	None
satdbg	Satellite tracking debug control	Command and enable/disable parameter	Command response	None	None
spoof	TCP acceleration control	Command and sub-command (and options if applicable)	Command response (and statistics if applicable)	None	None
stack	Protocol stack control	Command and sub-command (and options if applicable)	Command response (and statistics if applicable)	None	None
stats	Show global level stats	Command	Command response	None	None
stats (or net-stats)	Network stats	Command	Command response	None	None
status	System status report	Command	Command response	None	None
status	Network status report	Command	Command response	None	None
status	Remote or network status report	Command	Command response	None	None
TERMINATE	Kill process	Command and process	Command response	None	None
timer	Timer control	Command	Command response	None	None
tlev	Trace control	Command (and level if applicable)	Command response (and level if applicable)	None	None
tpdump	Dump timeplan	Command and enable/disable parameter	Command response	None	None
tunnel	Tunnel control	Command and sub-command (and options if applicable)	Command response (and statistics if applicable)	None	None
txodu	Remote ODU control	Command	Command response	None	None
txpower	Set remote tx power	Command and options	Command response	None	None
udp	UDP control	Command and sub-command (and options if applicable)	Command response (and statistics if applicable)	None	None

Service	Description	Input	Output	Key/CSP	Key/CSP Access
version	Display build information	Command	Command response	None	None
version	Display build information	Command	Command response and version information	None	None
vlan	Remote VLAN control	Command and sub-command (and options if applicable)	Command response (and statistics if applicable)	None	None
zeroize	Zeroize all critical security parameters at a global level, network level, or remote level	Command	Command response	All	Write

Table 6 – 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 a NetModem utilizing the OOB messages.

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 private key Key transport RSA public key	Read/write Read Read
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 7 – Client Crypto-Officer Services

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.

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 8 – Client User Services

Physical Security

The Protocol Processor is a multi-chip standalone cryptographic module. The evaluated platform is a production-grade rack-mountable IBM xSeries 335 server that includes a surrounding metal case. This case encloses all of the module's internal components and serves as the cryptographic boundary for the module.

The Protocol Processor 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 A (i.e., for business use).

Operational Environment

The Protocol Processor runs on a general purpose Operating System, Red Hat Linux version 7.3 and greater. The FIPS version of the Protocol Processor ships with the Linux operating system configured for single-user mode per CMVP guidance.

The testing of the module was performed using version 7.3 of Red Hat Linux.

Cryptographic Key Management

The Protocol Processor implements the following FIPS-approved algorithms:

- RSA (implemented in software) – PKCS#1 (vendor affirmed)
- SHA-1 (implemented in software) – FIPS 180-2 (certificate 220)
- Deterministic Random Number Generation (RNG) (implemented in software) – Appendix A.2.4 of ANSI X9.31
- Triple-DES CBC mode (implemented in hardware) – FIPS 46-3 (certificate 243)

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

- /dev/random RNG – for seeding the X9.31 RNG

The Protocol Processor 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 (using RSA encryption for key transport)	Volatile memory only (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 (hard drive - 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
Crypto-Officer role password	CSP	N/A	Non-volatile memory (hard drive - plaintext)	Authenticate the Crypto-Officer role
User role passwords	CSP	N/A	Non-volatile memory (hard drive - plaintext)	Authenticate the User role
X9.31 RNG seed and seed keys	Triple-DES (112 bits)	Internally generated by the /dev/random RNG (not used for data encryption)	Volatile memory only (plaintext)	Used by X9.31 RNG
Key transport RSA private key	RSA (2048 bits)	Internally generated using RSA key generation seeded with the X9.31 RNG	Volatile memory only (plaintext)	Key transport
Key transport RSA public key	RSA (2048 bits)	Internally generated using RSA key generation seeded with the X9.31 RNG	Volatile memory only (plaintext)	Key transport
Integrity check RSA public key	RSA (2048 bits)	Externally generated and hard-coded into the module's software	Non-volatile memory (hard drive - plaintext)	Software integrity check

Table 9 – Listing of Keys and CSPs

Triple-DES link encryption secret keys encrypt/decrypt Client User data traffic flowing between the Protocol Processor and an iDirect NetModem. These keys can either be statically configured or dynamically generated. When dynamically generated, the initial link encryption keys are loaded onto the module by the Client Crypto-Officer (RSA encrypted) and subsequent dynamic keys (i.e., for re-keying or multicast traffic) are generated internally by the Protocol Processor. 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 (hard drive).

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.

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 (hard drive).

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

The key transport RSA private key is generated internally by the module and is used for key transport during dynamic keying for link encryption. This key is stored in volatile memory in plaintext.

The key transport RSA public key is generated internally by the module and is used for key transport during dynamic keying for link encryption. This key is stored in volatile memory.

The integrity check RSA public key is hard-coded into the module's software. This key is externally generated and verifies the integrity of the module's software image during power-up. This key is stored on the module's hard-drive in plaintext.

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

Self-Tests

The Protocol Processor performs the following self-tests at power-up:

- Software integrity check – RSA digital signature over all of the module's software
- Known Answer Tests (KATs)
    - Triple-DES
    - SHA-1 HMAC
    - X9.31 RNG

The Protocol Processor performs the following conditional self-tests:

- Continuous RNG tests for the X9.31 RNG and the /dev/random RNG whenever the RNG's generate random data.
- Manual key entry test whenever Triple-DES 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.
- RSA encrypt/decrypt pairwise consistency check whenever RSA key pairs are generated.

If either of the power-up self-tests, the continuous RNG tests, or the pairwise consistency check fails, 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 fails, 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 Protocol Processor does not employ security mechanisms to mitigate specific attacks.

SECURE OPERATION

The Protocol Processor 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 ports. 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 must not take the module's Operating System (OS) out of single-user mode. This generally means that the OS configuration (i.e., only a root account, no remote access OS daemons) of the Protocol Processor as received from iDirect may not be modified. Additionally, the Crypto-Officer must not modify the configuration files for the module directly through OS calls.

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 Protocol Processor's logs and other status information to ensure the module is functioning properly. If the Protocol Processor 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 private and secret keys, and CSPs.

User Guidance

The User is responsible for non-security-relevant management of the module through the 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 6 above).

The User should routinely check the Protocol Processor's logs and other status information to ensure the module is functioning properly. If the Protocol Processor 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 are entered into or output from the module in an encrypted form.

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 use the module securely.

ACRONYMS

ANSI	American National Standards Institute
API	Application Programming Interface
ARP	Address Resolution Protocol
C2T	Cable Chaining Technology
CD-ROM	Compact Disk Read Only Memory
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
CVS	Concurrent Versions System
DES	Data Encryption Standard
EDC	Error Detection Code
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
HMAC	(Keyed-) Hash Message Authentication Code
IP	Internet Protocol
ISM	Integrated System Management
KAT	Known Answer Test
LED	Light Emitting Diode
NIST	National Institute of Standards and Technology
OOB	Out Of Band
OOBC	Out Of Band Chunks
OS	Operating System
PAD	Packet Assembler / Disassembler
PKCS	Public Key Cryptography Standards
QoS	Quality of Service
RNG	Random Number Generator
RSA	Rivest Shamir and Adleman
SAR	Segmentation and Reassembly
SHA	Secure Hash Algorithm
TCP	Transport Control Protocol
USB	Universal Serial Bus
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VSAT	Very Small Aperture Terminal
VSS	Visual Source Safe

