Port Authority 44

Cryptographic Module Security Policy

Rev. 1N February 24, 2005

Communication Devices Inc.
One Forstmann Ct.
Clifton, NJ 07011
USA
Phone: 973 772 6997
Fax: 973 772 0747
Internet: support@commdevices.com

Table of Contents

Table of Figures

Tables

1 Introduction

1.1 Scope

This document sets forth the security rules under which the Port Authority 44 cryptographic unit will operate, including rules derived from FIPS 140-2.

1.2 FIPS 140-2 Table of Security Levels

Security Requirements	FIPS 140-2 Security Level
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	3
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self Tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A
Overall Level	2

Table 1-1 FIPS 140-2 Table of Security Levels

1.3 Related Documents

- Port Authority 44 Manual
- Front End Loader Manual
- FCC Test Report
- Finite State Machine

1.4 Glossary

ANSI	American National Standards Institute
FIPS 171	KEY Exchange Standard
CSM	Cryptographic Service Module
DES	Data Encryption Standard
EIA RS232	Modem/Host Interface
EIA RS232 Signals	DCD Data Carrier Detect DTR Data Terminal Ready RTS Request to Send CTS Clear to Send GND Signal Return (Ground) DSR Data Set Ready TxD Transmit Data RxD Received Data
Front End Loader	CDI Software to manage Port Authority Units
NIST	National Institute of Standards and Technology
PC	Personal Computer
PIN	Personal Identification Number
PTSN	Public Telephone System Network
VAC	Voltage Alternating Current
VAC CT	Voltage Alternating Current, Center Tapped
WAN	Wide Area Network
LAN	Local Area Network
RADIUS	Remote Authentication Dial-In User Services
TACACS	Terminal Access Controller Access Control System

1.5 Out of Band Management

Out of Band Management refers to products that permit secured technician access to "Network Elements" (firewall, routers, bridges, sonet switches, servers etc.) via dial up telephone lines (not in the bandwidth of the network). By far, SNMP (the Simple Network Management Protocol) network management is the industry choice for managing wide area and local area networks. This is In Band Management access via the network. SNMP is easy to use and inexpensive. It has however one inherent weakness: SNMP management information travels the same network path as the data. It uses the same WAN and LAN routers, hubs and communications links. Communication is subject to interception and the same problems that the network is currently having. When the network goes down or is severely disrupted, SNMP traffic has no way to get between the managed device and the management workstation. Quite often when a "Network Element" goes down, it loses its network connection, which renders In Band Management useless. This is where the Port Authority module always works flawlessly for Out Of Band Management.

1.6 Port Authority 44 Application

The Port Authority 44 is designed to protect firewall/router console port access. The device was designed to overcome the weaknesses of RADIUS and TACACS+ for remote access authentication. The problem of the firewall/router not being able to contact the RADIUS or TACACS+ server is eliminated by the Port Authority 44 which stores its own database of up to 150 users right on board!

The Port Authority 44 supports speeds up to 115.2 Kbps and has a built in V.34 internal modem and can be managed by the CDI's Front End Loader.

Full Triple-DES encryption is supported when communicating with CDI's FIPS 140-1 validated UniGuard V34.

1.7 Block Diagram of Hardware Components

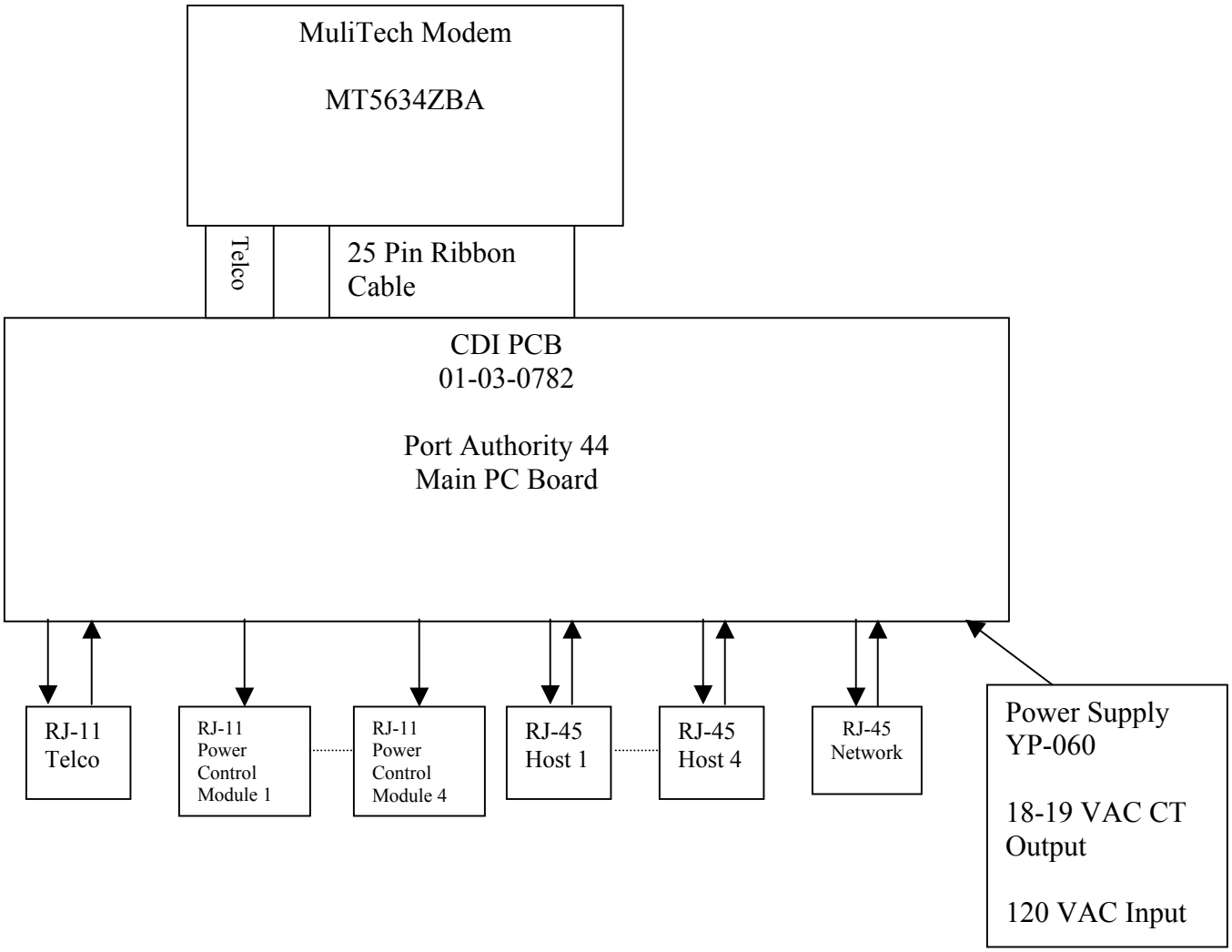

Figure 1-1 *Block Diagram of Hardware Components*

1.8 PA-44 Revision Levels

The following are the validated version numbers for the hardware and firmware.

Hardware version 01-03-0782
Firmware version 2.15

2 Description of Cryptographic Boundary

The cryptographic boundary for the Port Authority consists of several components. The Port Authority consist of a modem, a Power port, a Network port, -four RJ45 Host ports, four Power Control Module ports and I/O Modules. The firmware consists of component parts such as the Encryption Chip, the User Authentication Module, the DataBases, the Host Buffer, and the Modem Buffer. Figure 2-1 below shows how the different components fit together. The following sections provide discussions on each component.

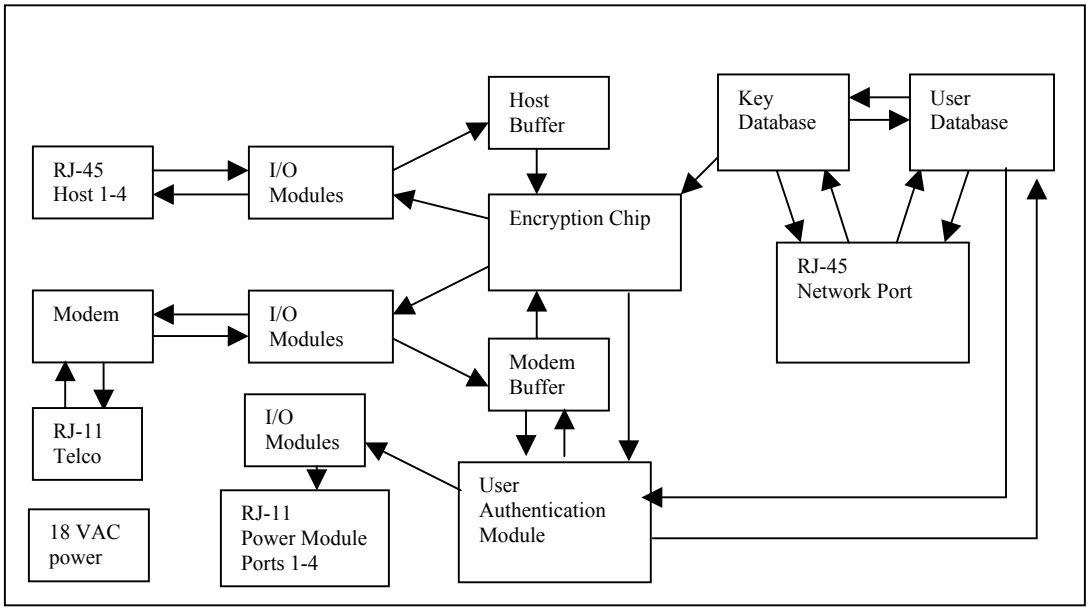

Figure 2-1 *Cryptographic Boundary*

2.1 Host Port RJ-45

The Host Ports on a Port Authority connects to equipment that needs security protections over a PTSN, such as Firewalls, Routers, and Switches. Clear text data moves in/out of Port Authority through each of the four (4) RJ-45 connectors labeled Host. Each RJ-45 port has the following signals for EIA-RS232 interface with the RJ-45 cable and DB-25 connector. The signals are DCD, DTR, RTS, CTS, GND, DSR, TxD, and RxD.

2.2 Modem / RJ-11

Operator authentication data, plain text data, and encrypted data move in/out of the Port Authority through the Modem port. The RJ-11 provides a standard 2 wire or 4 wire Telco interface to connect to Public Telephone System Network (PTSN).

2.3 I/O Modules

The I/O Modules read and write data to the UART. Data read from a port is buffered in a circular buffer for the other modules. When a module is in control it will remove the data from the buffer. The two modules that remove data from the buffer are the User Authentication Module and the Encryption Chip.

2.4 Power

Power requirements are 18-19 VAC with center tap.

2.5 User Authentication Module

The User Authentication Module will read data from the Modem Buffer to authenticate the operator. If the User ID is correct the User Authentication Module will initiate the Encryption Chip. After the Port Authority is in Encrypted mode using FIPS 171 key exchange, it will prompt and check to see if the password is correct for this User. This prevents passwords from being sent in the clear. If the password is correct for this User, the Port Authority will pass control back to the Encryption Chip for encrypting/decrypting data with Triple-DES.

The User ID and keys must be loaded in the Port Authority by the Crypto-Officer prior to a operator authentication else the operator will be denied access and re-prompted to enter an ID. After three unsuccessful attempts the Port Authority will disconnect the call.

2.6 Encryption Chip

The Encryption Chip implements the Triple-DES algorithm for encryption and decryption of data.

2.7 Network Port

The Network Port of the module connects to a PC and is used to manage and configure the Port Authority using the Front End Loader graphical user interface (GUI) package. The Front End Loader is CDI's proprietary software program that resides on a PC. With the Front End Loader, the Crypto-Officer will be able to change the system parameters such as the host port speed, data bits, parity, time and date, Crypto-Officer password, add/delete/modify Users and cryptographic keys. The Crypto-Officer will also be able to review and delete the audit trail activity of Users with the Front End Loader program.

2.8 DataBases

The Databases contain the following items: port parameters, which includes data bits, baud rate hardware flow control, the keys, and the operators' information such as User IDs and passwords.

2.9 Host Buffer

The Host Buffer is circular buffer that holds clear text data input from a Host port that's being accessed. This buffer is read by the Cryptographic Module to encrypt data using Triple-DES before it is sent out the Modem port.

2.10 Modem Buffer

The Modem Buffer holds plain text and Triple-DES encrypted data that is input from the modem. The Cryptographic Module will decrypt encrypted data before being sent out the Host port that is accessed.

2.11 Power Control Modules

Power Control Modules are remote to the Port Authority 44. These modules are used to recycle (turn off then turn on) the power of remote devices that may have become inoperative. This will reset the device and usually restore operation. Power Control Modules can also be used to shut down (turn off the power to) a device that should not be operating. The module can also be used to restore power to a device that has been turned off. The Power Control Modules are controlled by signals sent from the Port Authority 44.

The rear panel of the Port Authority 44 contains four ports labeled Power Control Modules. Each port can control a single remote Power Control Module.
The Port Authority 44 is connected to the Power Control Modules with a cable, containing and RJ-11 connector on each end. One end of the cable is inserted into the RJ-11 receptacle (Power Control Module port) located on the rear of the Port Authority 44 and the other end of the cable is inserted into the RJ-11 receptacle located on the remote Power Control Module.

3 Physical Security

3.1 Physical Embodiment

The multi-chip stand-alone cryptographic module consists of a number of IC chips mounted on a printed circuit board contained within a protected enclosure. The enclosure contains tamper seals that will destruct if an attempt is made to remove them.

Figure 3-1 *Port Authority 44 with 2 Tamper Seals*

3.1.1 Tamper Seals

Four (4) tamper seals cover the two (2) screws that fasten the top cover to the front panel and two (2) screws to the top and bottom panels. If any attempt is made to remove the top cover these screws must be removed first. Removing these screws will destroy the tamper seals.

3.1.1.1 Front Tamper Seals

The front tamper seals (2) are shown in figure 3-1. These seals prevent removing the top cover form front panel without damaging the seals. These seals cover the screws (2) that fasten the top cover to the front panel. When a seal has been damaged it indicated that the unit might have been tampered with.

3.1.1.2 Rear Tamper Seals

The rear tamper seals (2) are shown in figure 3-2. These seals prevent removing the top cover form the chassis base without damaging the seals. These seals cover the screws (2) that fasten the top cover to the chassis base. They cover the screws as well as wrap around the top cover and also connect to the chassis base. When a seal has been damaged it indicated that the unit might have been tampered with.

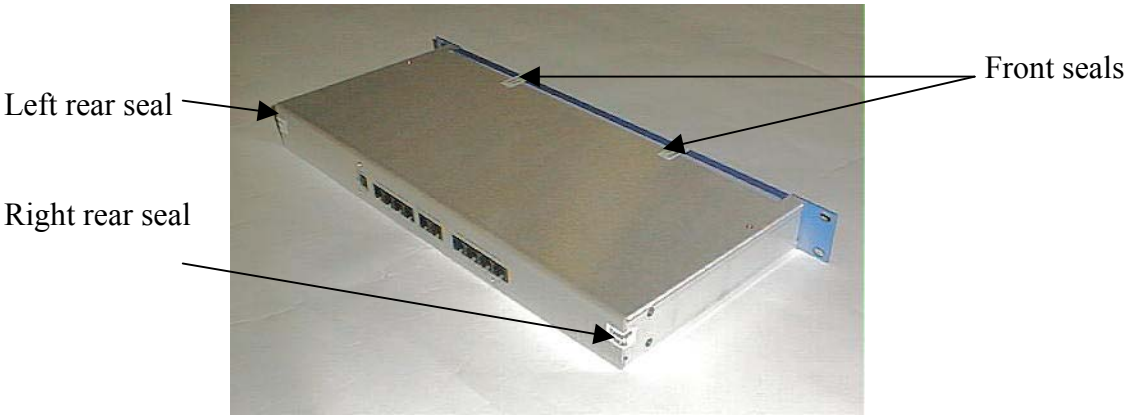

Figure 3-2 *Rear Tamper Seals*

3.1.2 Tamper Switches

The circuit board contains two tamper switches. The rear tamper switch will trip if an attempt is made to remove the top cover. The top cover must be removed in order to remove either the front panel or the chassis base. The front tamper switch will trip if an attempt is made to remove the front panel.

If either of these tamper switches are tripped, the RAM containing all keys and User information will be zeroed. The zeroization circuit will activate regardless if the unit is powered by battery back up or powered by AC.

All IC chips are standard circuits.

3.1.3 The Modem Board

The multi-chip cryptographic module printed circuit board has the modem mounted on top of the board.

3.2 Enclosure

The enclosure, shown not assembled below in Figure 3-3, consists of a front panel, a bottom chassis, and a Top Cover.

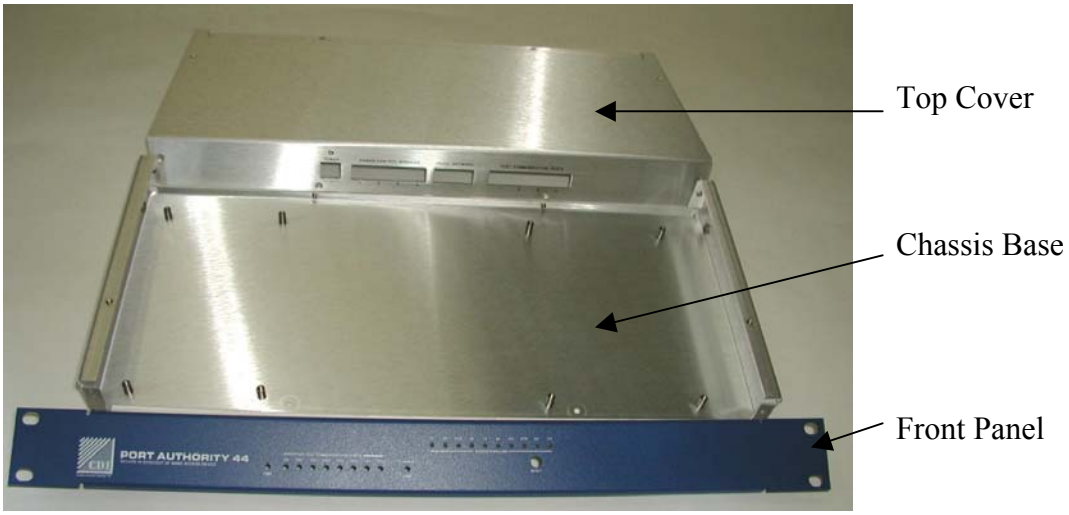

Figure 3-3 Enclosure, not assembled.

3.2.1 Front Panel

The front panel is 19.00 inches wide, by 1.720 inches high and 0.079 inches thick. The panel contains a top and bottom lip each containing two (2) PEM nuts used to fasten the panel to the chassis base and top cover. The top lip is 0.500 inches deep and the bottom lip is 0.848 inches deep

The front panel is fastened to the chassis base by two (2) screws and to the top cover by two (2) screws. To remove the front panel, both sets of these screws must be removed. To remove the top cover, the two (2) screws that fasten the top cover to the front panel must be removed.

3.2.2 Top Cover

The top cover is 16.800 inches wide and 7.765 inches deep. The cover is L shaped with the L portion 1.700 inched long. This provides room for the connector cutouts located on the rear of the assembled unit.

The top cover is inserted under the front panel lip and fastened to the front panel with two (2) screws. There are also two (2) screw holes located on the top of the top cover which have two (2) screws inserted into Pem Nuts on the chassis base top flange. There are four (4) additional screws located on the rear of the top cover that are fastened to the rear of the chassis base.

3.2.3 Chassis Base

The chassis base is 16.800 inches wide by 7.707 inches deep. The base is U shaped with the sides of the U being 1.642 inches high. These sides are reinforced with a lip 0.500 inches wide, which allow for the PEM nuts that secure the front panel and top cover.

4 Roles And Services

4.1 Crypto-Officer Role

The Port Authority supports only one Crypto-Officer for the purpose of programming Port Authority. The default password for the Crypto-Officer is set at the factory. The Crypto-Officer will use the Front End Loader, a Windows package for programming purposes. The Crypto-Officer will connect the serial port of the PC to the port labeled Network on the Port Authority. This is the only port that can be used to program and/or modify the Port Authority.

With Front End Loader the Crypto-Officer will be able to change the system parameters such as the Host port speed, data bits, parity, set time and date, change the Crypto-Officer password, perform firmware upgrades, add/delete/modify Users and cryptographic keys. The Crypto-Officer will be able to review and delete audit trail activity of Users with a CDI Front End Loader program.

4.2 User Role

A User does not have access to the Network port of Port Authority that is used by the Crypto-Officer. The User only has access to the modem and Host ports through the cryptographic module of Port Authority. To gain access to the Host port the User must first authenticate himself through the modem, and Port Authority must enter encryption mode. Once he has authenticated he will be granted access to the Host port. A User needs at minimum an ID and password to authenticate in Port Authority's database. Along with the User ID and password, keys must have been loaded in the Port Authority database for the remote device.

4.3 Services

The services that Port Authority provides are (see Table 4-1)

Cryptographic operations
Encryption – Port Authority will encrypt the data with Triple-DES before sending it out the Modem port to the PTSN. The purpose is to secure the data to protect against unauthorized viewing and/or use.

Decryption - Port Authority will decrypt the data with Triple-DES that it receives from PTSN through the Modem port and deliver the data to the equipment connected to the Host port. To be able to use the data that was sent from a remote module, it first has to be decrypted so that it is in usable form for the end User.

Bypass – Port Authority can send and receive clear text data through the Modem port when operating in the Bypass (clear text) mode. The purpose of this mode is when security of data is not needed. This occurs when security is disabled in the Unit.

Message integrity - Port Authority uses the Triple-DES MAC function that is part of the FIPS 171 – Key Management Using ANSI X9.17 standard to protect against attack of the key exchange.

Audit Log – Port Authority logs date/time of every access made by Users as well invalid attempts.

Firmware Load – Port Authority allows a Crypto Officer to update the firmware in the devices. The integrity of the code is checked by using a Triple-DES MAC.

	Roles and Services				
Operator	Encryption/ Decryption	Bypass	Message integrity	Audit Log	Firmware Load
User	X	X	X		
Security Officer		X		X	X

Table 4-1 Roles and Services

4.4 Critical Security Parameters

The table 4-2, below, shows the Critical Security Parameters that are stored in the Port Authority's tamper protected RAM and the roles that have access to them:

CSP	Access (CO Role)	Type of Access for CO (Read, Write, Execute)	Access (User Role)	Type of Access for User (Read, Write, Execute)
User IDs	X	R,W,E	X	E
Passwords	X	R,W,E	X	W,E
System Key	X	R,W,E	-	-
Encryption Keys	X	R,W,E	X	E
Session Keys	-	-	-	-
Triple-DES MAC Keys	X	R,W,E	-	-
Triple-DES MAC Integrity Key	-	-	-	-
Seed Keys	X	R,W	-	-
RNG	-	-	-	-
IVs	-	-	-	-

Table 4-2 Critical Security Parameter (CSP)

4.5 Management Functions

Audit – Port Authority saves up to 150 transactions for review by the Crypto-Officer with Front End Loader. Port Authority saves time/date, the User that authenticated, and any attempts from an unauthorized User.

4.6 Operator Authentication

The Port Authority by default will not authenticate and or operate in the clear text mode until the unit has been programmed with operators, ID's, keys and system parameters. If an external operator dials into the Port Authority with a remote FIPS 140-1 validated UniGuard V34, the operator will be prompted for an ID and password. If an invalid ID or Password is entered, the operator will receive an invalid ID/Password message. This message does not tell the operator what was invalid. The operator will be prompted for an ID and password again. After three invalid attempts the call will be disconnected. This will only allow a maximum of three attempts within a minute.

The default password should be changed after the Crypto-Officer gains access and to prevent further access to the Port Authority programming menu of the Front End Loader using this default.

If an Operator has been authenticated and the unit is powered down and then powered back up, the authentication session is terminated. When power is lost, the modem will automatically disconnect from the phone line. The Operator will be required to dial in and authenticate again after the unit is powered up.

4.7 Identity Based Authentication

Port Authority provides identity-based authentication. The operator must enter an ID and password or some other form of challenge and response. If the User ID and password are valid, the operator will cause the Port Authority to start encryption and authentication with the remote hardware. For the strength of authentication, the module passwords must be at least 6 characters long. These are alphanumeric characters as well as keyboard/extended characters, which gives a total of 95 characters to choose from. A 6-character password using all uppercase letters has a total possible combination of 26^6 = 308,915,776. Therefore the probability for a random attempt to succeed is less than one in 1,000,000. In FIPS mode, the module implements a delay of at least 10 seconds after each incorrect entry of a password. In FIPS mode, the module locks out an operator after 3 unsuccessful attempts at entering a password. Therefore the associated probability of a successful random attempt during a one-minute period is less than one in 100,000.

If a password is used, it is masked during entry. Star symbols are displayed during entry of the authentication data to mask the original content. For Challenge/Response the response is encrypted. This provides no information that could be used to guess or determine the authentication data. The following figure 4-3 shows how operators can be authenticated.

	Authentication Mechanisms		
Role	Challenge/Response with complete session encryption	Challenge/Response with a token	Challenge/Response without a token (bypass)
User	X	X	X
Crypto-Officer	X	X	X

Table 4-3 Authentication Mechanisms

4.8 Types of Users

4.8.1 Encryption User

4.8.1.1 UserID/Password User

An Encryption, CallBack, or Pager User will be assigned a User ID/password as well as a six character numeric ID and secret key of the remote UniGuard. The User ID will be in the clear while the password will be sent encrypted with Triple-DES.

An example of Challenge/Response with complete session encryption involves a User that is prompted (Challenge) for a 6-character User ID and 6 to 8-character password. The User enters the information (Response) and attempts to log into a remote Port Authority using a local UniGuard-V34 device. Once the User has sent the User ID in the clear, the Port Authority generates a unique session key. The module looks up the User's encryption key based on the ID entered. The session key is sent encrypted using FIPS 171 with Triple-DES to the User using that encryption key. If the User has the proper encryption key at the local unit, the session key can be decrypted and used to send the User password to complete the authentication. If both the User ID and password are valid, the rest of the session will be encrypted using Triple-DES and the User gains access to the Port Authority and the host PC connected to it.

4.8.1.2 Token User

A Token User has in his or her possession a token, which will aid in assuring that the person using the equipment is the person assigned to the token. Types of Tokens are SecureID Token, DPI Token and CryptoCard Token.

An example of Challenge/Response with a SecureID token involves an operator that has possession of an external token device. The token contains a time clock together with a User's encryption key. The key is used to encrypt the time, which is displayed in the LCD of the token. The User is prompted (Challenge) for the User ID and the encrypted displayed information when logging on. After entering this information (Response), the module looks up the user's encryption key and compares the encrypted information to the information generated by the module with the User's encryption key. A session key is generated by Port Authority using the ANSI 9.31 PRNG and sent encrypted to the User using that encryption key. If the User has the proper encryption key at the local unit, the session key can be decrypted and the User then sends his/her password to complete the authentication. If both the User ID and password are valid, the rest of the session will be encrypted and the User gains access to the Port Authority and the host PC connected to it.

4.8.2 User with or without Encryption

These Users can authenticate and pass data in the clear unless they have been assigned to use encryption. After they authenticate to the Port Authority, they can use it's keys.

An example of Challenge/Response without a token involves an operator that is prompted for a User ID and password from the remote Port Authority module. The operator enters the authentication information and is granted access if it is correct. This occurs when the module is operating in the bypass mode and neither the authentication process nor the session is encrypted.

5 Operational Environment

The Port Authority uses a limited operational environment. The code that is executed in the Port Authority does not employ an Operating System, and the code is stored in a FLASH chip in binary executable format. An operator cannot add/delete/modify the existing code in the Port Authority.

Use of the cryptographic module is limited to a single User at a time.

The Port Authority only provides for one User connection at a time, because the User must authenticate through the single modem to gain access to the Cryptographic Module. Only the data that flows through Port Authority between the Modem and Host ports employ the Cryptographic Module. Any other User attempting to dial in to the Port Authority will receive a busy signal. Port Authority allows authentication through the Network Port by the Crypto-Officer when the modem is not in use.

Use of the cryptographic module is dedicated to the cryptographic process during the time the cryptographic process is in use.

By the statement above it is impossible to have multiple operators connected to the Port Authority at the same time because the Port Authority only interfaces to the PTSN with only a dialup modem, and the PTSN only allows for one connection per dialup circuit.

6 Key Management

Key and Parameter entry – All keys and parameters with the exception of the Integrity key, Seed keys, and Session keys can be entered into Port Authority through the Front End Loader Windows package in clear text. The PC that the Front End Loader is installed on is standalone and is not connected to a network. The PC is considered to function as a key loader.

Key output – Only Session and Triple-DES MAC keys can be output encrypted. These keys are wrapped with the Triple-DES Encryption keys before they are output. The review of the keys that have been entered will not be possible. The System key, Key Encryption Keys, and Seed keys are displayed in clear text through the Front End Loader Windows package.

Key zeroization – When the unit is physically opened up, there are tamper switches that will cause a short across SRAM, (removing Vcc and replacing it with a short to ground) which in turn will zero out, reset the SRAM to all bytes of ram to 0xff which includes keys and parameters. SRAM is battery backed up to save the keys and User data stored within SRAM. Only the Integrity key and default System key that are hard-coded into the firmware would not be zeroed out. These keys can only be zeroized by erasing or overwriting the firmware.

Key generation – The key generation process for creating the Seed and Session keys uses the ANSI X9.31, Appendix A pseudo-random number generator.

6.1 Key Storage

Keys are stored in a packed BCD format in the Port Authority's battery backup RAM. If power is lost to RAM and the batteries are dead, the keys will be zeroed out. The battery circuitry includes two tamper switches, one located behind the front panel and the other behind the rear panel. If one of these switches is tripped by removing the front or rear panel, the keys will be destroyed. Pack BCD allows for 2 plain text characters to be stored in a byte so each one of the 16 plain text character keys are stored in 8 bytes of RAM. Triple-DES requires 3 keys or 24 bytes of RAM.

The seed keys can't be changed once they are loaded into Port Authority.

An ID and key will be assigned to a Port Authority for a remote User. When this is done, only that key and ID can be used to connect to a Host Port Authority with encryption. If the key or the ID is incorrect, the Port Authority will drop the connection after 3 attempts. Each User has an ID, password and encryption key to gain access to the Host port of Port Authority.

All keys that are used for a cryptographic session between Port Authority 44 and UniGuard V34 are generated by the Port Authority. The key generation process for creating the keys uses ANSI X9.31 Appendix A pseudo-random number generator to create the Triple-DES keys. The keys are distributed by using FIPS 171 – Key Management Using ANSI X9.17 key management with the use of Triple-DES MAC keys.

6.2 Key Archiving

Port Authority does not provide a means of retrieving keys for archiving purposes.

	Key Management			
	Triple-DES MAC	Key Zeroization	ANSI X9.31	FIPS 171
Private Key	X	X	X	
Session Key	X	X	X	X
RNG		X	X	X

Table 6-1 Key Management

7 Cryptographic Algorithms

The cryptographic algorithms used in the Port Authority are Triple-DES and ANSI X9.9 Triple-DES MAC as referenced in FIPS 171.

8 FCC Approval

Port Authority is FCC approved for Part 15 Class A.

9 Self Tests

The self-tests are run every time Port Authority is powered up and upon certain conditions (session key generation via ANSI X9.31 random number generator, a test is continuously run for this after power up self test). The self-test does not alter the contents of Port Authority. The device performs the following tests:

Power Up Tests

- Triple-DES Known Answer Test
- Firmware Integrity ANSI X9.9 – Triple-DES MAC Calculation Test
- Random Number Generator Known Answer Test

Conditional Tests

- Bypass Test
- Firmware Load ANSI X9.9 – Triple-DES MAC Calculation Test
- Continuous Random Number Generator Test

10 Design Assurance

10.1 Design

The Port Authority-44 is a Secure 4 port switch that allows a single internal dial up modem to access up to four (4) remote devices and also control signals for four Power Cycle Modules.

10.2 Configuration Management

Configuration Management for Port Authority consist of the Port Authority Security Policy, User Manual Rev 1-103D, Front End Loader Program Version 2.14B and Manual, and the Port Authority Firmware Version 2.14.03.

Hardware and Software changes and updates are handled though Revision Control and Engineer Change Notice (ECN). An ECN is issued only after test engineering performs a complete test.

Deployment and Installation Communication Devices Inc. (CDI) tracks each shipment and is able to provide confirmation to the customer that a Port Authority 44 Cryptographic Module has been received.

For a secure installation of the Port Authority, it should be installed in the same secured area as the equipment that will be connected to Port Authority host ports. Installation must be performed according to the instructions in the User Manuals. When the module powers up, the self-tests are automatically run. If all tests pass, the module is available to be initialized and perform cryptographic functions. After Port Authority is installed with the Front End Loader program, the Crypto-Officer is able to load keys, User ID's, passwords, and change the default pre-programmed password in the Port Authority.

11 Security Policy Rules Of Operation

Port Authority 44 is designed and meets FIPS 140-2 Level 2 requirements for hardware and software functionality.

To gain access to the host device that Port Authority is protecting, the Port Authority must be in a cryptographic mode such that all data in/out of the modem to the PTSN is encrypted with Triple-DES. The User must be programmed in the database and has rights to the host port of Port Authority. Each User first has to be authenticated before Port Authority goes into cryptographic mode.

A host Port Authority will only authenticate in the cryptographic mode with a client UniGuard that has the same six-character numeric ID and keys that's in its own database.

All data in/out of Port Authority for programming User ID's, Keys, Port Parameters, and Device Options will be clear text.

The firmware can be updated in the Port Authority by over writing the existing FIPS 140-2 validated firmware with a new version of FIPS 140-2 Validated firmware. The update uses ANSI X9.9 – Triple-DES MAC Calculation Test when updating the firmware.