FIPS 140-2 Security Policy

Rev 1.24 October 2011

Port Authority Series

Firmware Version: 10.00.78
Hardware Version:

PA111-SA CDI 01-03-0912B

PA111-RM CDI 01-03-0912B
PA155-RM CDI 01-03-0912B
PA199-RM. CDI 01-03-0912B

Communication Devices Inc.
85 Fulton Street.
Boonton, NJ 07005
Tel: 973 334 1980
Fax: 973 334 0545
Internet: support@commdevices.com

FIPS 140-2 Non-Proprietary Security Policy

Table of Contents

Table of Figures

Table of Tables

1 Introduction

1.1 Scope

This document sets forth the security rules under which the Port Authority cryptographic units will operate, including rules derived from FIPS 140-2.
For more information, please refer to the Federal Information Processing Standards Publication 140-2, available on the NIST website:
http://www.nist.gov/itl/upload/fips1402.pdf

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 1.2-1 Table of Security Levels

1.3 Related Documents

- Port Authority 111/155/199 Manual
- Front End Loader Manual
- FCC Test Report
- Finite State Machine

Glossary

AES	Advance Encryption System
ANSI	American National Standards Institute
ASCII	American Standard Code for Information Interchange
CDI	Communication Devices, Inc.
CO	Crypto-Officer
CSM	Cryptographic Service Module
DRAM	Dynamic Random Access Memory
EIA/RS232	Modem/Host Serial 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 Application to manage Port Authority Units
Flash	Flash Solid State Memory
FPGA	Field Programmable Gate Array Integrated Circuit
HMAC	Hash-based Message Authentication Code
KAT	Known Answer Test
Kbps	Kilo Bauds per Second
Mbps	Mega Bits per second
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology

OBM	Out of Band Management
PA	Port Authority
PC	Personal Computer
PCB	Printed Circuit Board
PCM	Power Control Module
PTSN	Public Telephone System Network
RM	Rack Mounted
RNG	Random Number Generator
RTC	Real Time Clock
RTOS	Real Time Operating System
SRAM	Static Random Access Memory
SA	Stand Alone
VAC	Voltage Alternating Current
VDC	Voltage Direct Current
WAN	Wide Area Network
LAN	Local Area Network
RADIUS	Remote Authentication Dial-In User Services
SNMP	Simple Network Management Protocol
TACACS	Terminal Access Controller Access Control System
UART	Universal asynchronous receiver/transmitter

1.4 Out of Band Management (OBM)

Out of Band Management refers to products that permit secured technician access to "Network Elements" (e.g. Firewalls, Routers, Bridges, SONET, Switches, Servers etc.) via dial up telephone lines (not in the bandwidth of the network). By far, SNMP 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 OBM. To augment the Port Authority usefulness, access to network is available.

1.5 Mode of operation

The Port Authority has 2 modes of operation:

1. FIPS mode

The Enable Security mode is a FIPS mode. In this mode the communication between an operator and the Port Authority is fully protected by encryption, and user authentication is enabled.

2. Non-FIPS mode

The No Security/Bypass mode is a non-FIPS mode. In this mode the communication is in clear text and user authentication is disabled. The Port Authority does not contain any keys or CSPs.

1.6 Port Authority Application

The Port Authority is designed primarily 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 which stores its own database of up to 150 users right on board!

The Port Authority supports speeds up to 115.2 Kbps and has a built-in V.92 internal modem and can be managed by the Front End Loader.

AES encryption is supported when communicating with other CDI's FIPS 140-2 validated Port Authority.

1.7 Block Diagram Hardware Components

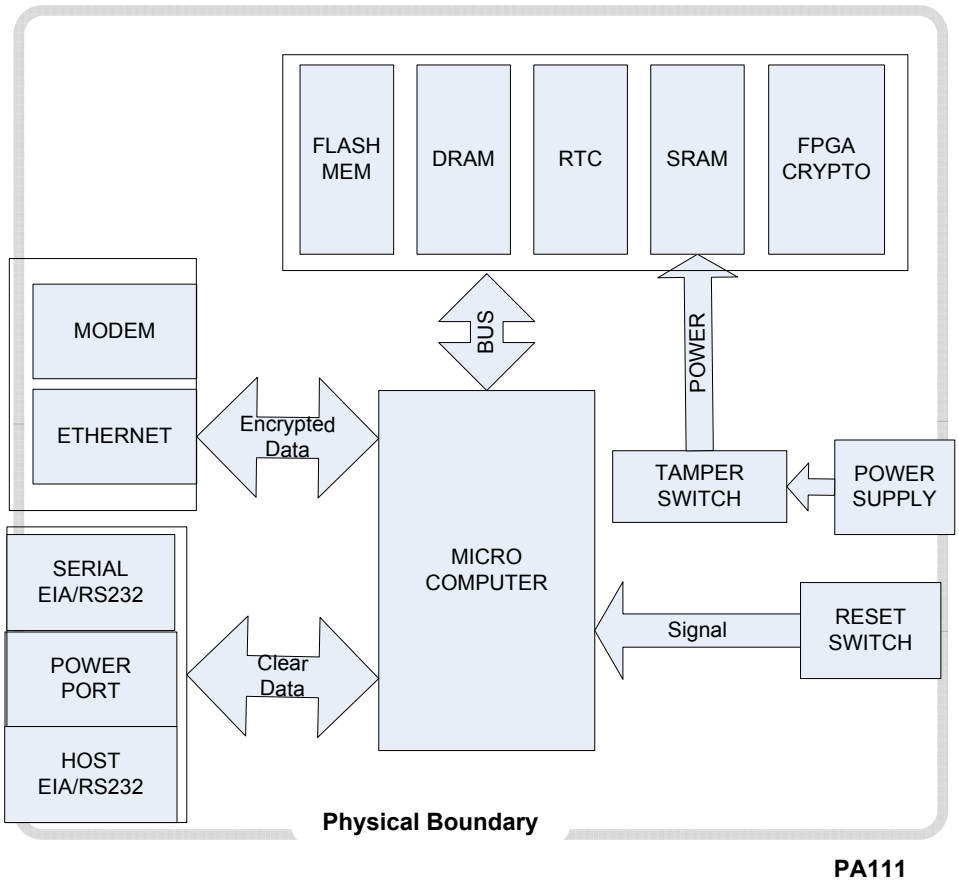


Figure 1-1 PA111 Hardware Diagram

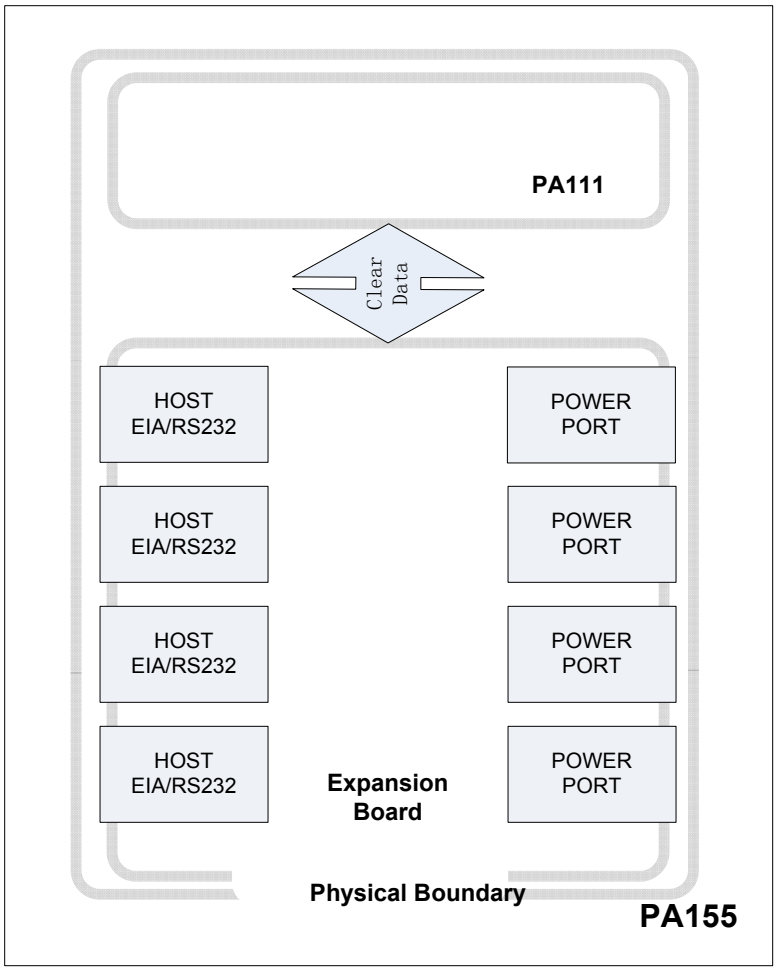


Figure 1-2 PA155 Hardware Diagram

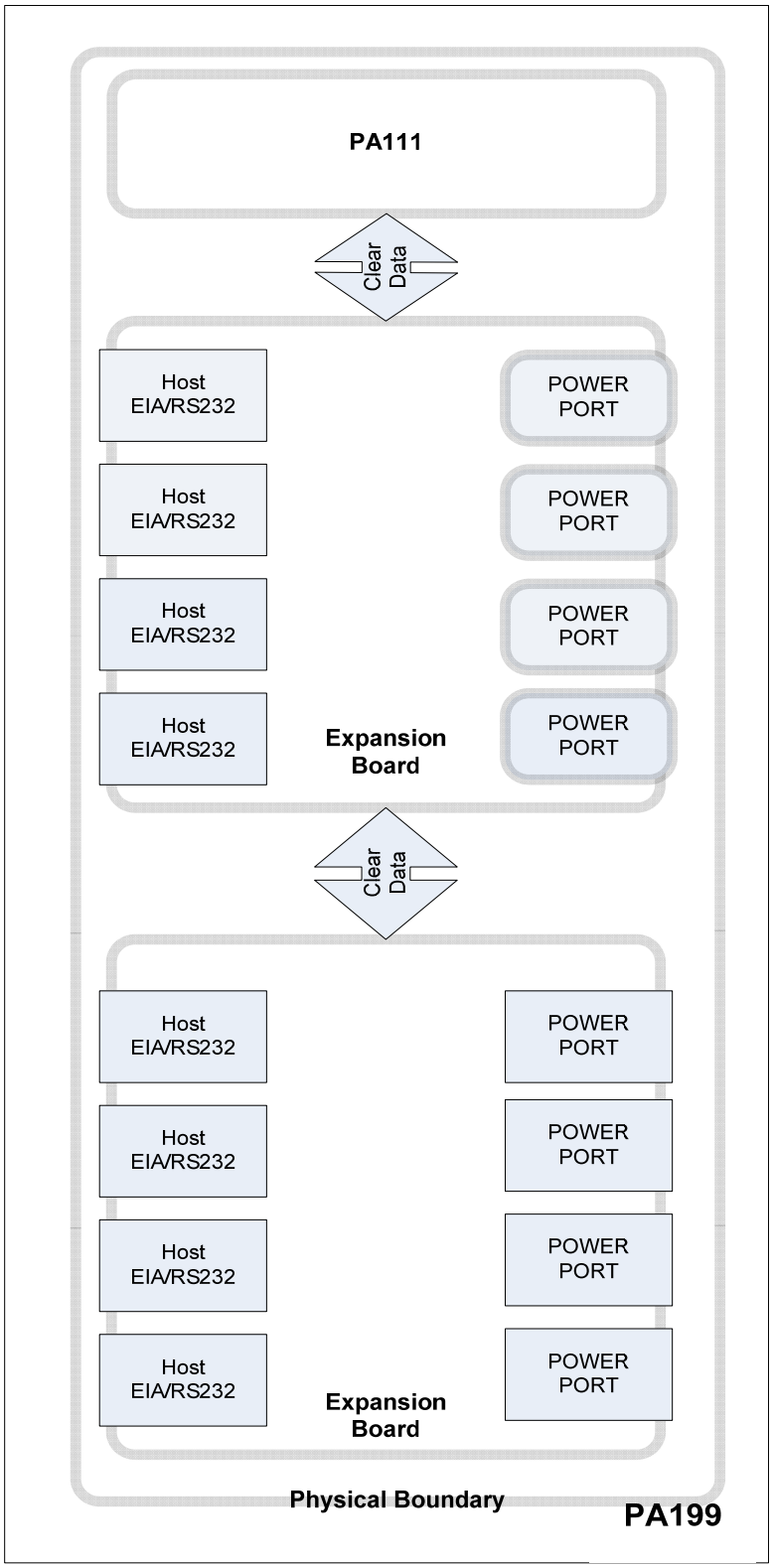


Figure 1-3 PA199 Hardware Diagram

1.8 PA Revision Levels

The following are the validated version numbers for the Hardware and Firmware.

Hardware version 01-03-0912 B
Firmware version 10.00.78

2 Description of Cryptographic Boundary

The enclosure defines the cryptographic boundary of the module.
The cryptographic boundary for the Port Authority consists of several components. The Port Authority consists of a modem, a Power port, a Network port, RJ45 Host ports, ports and I/O Modules. The firmware consists of component parts such as the Encryption Module, the User Authentication Module, the Databases, and the interface Buffers. Figure 2-1 below shows how the different components fit together. The following sections provide discussions on each component.

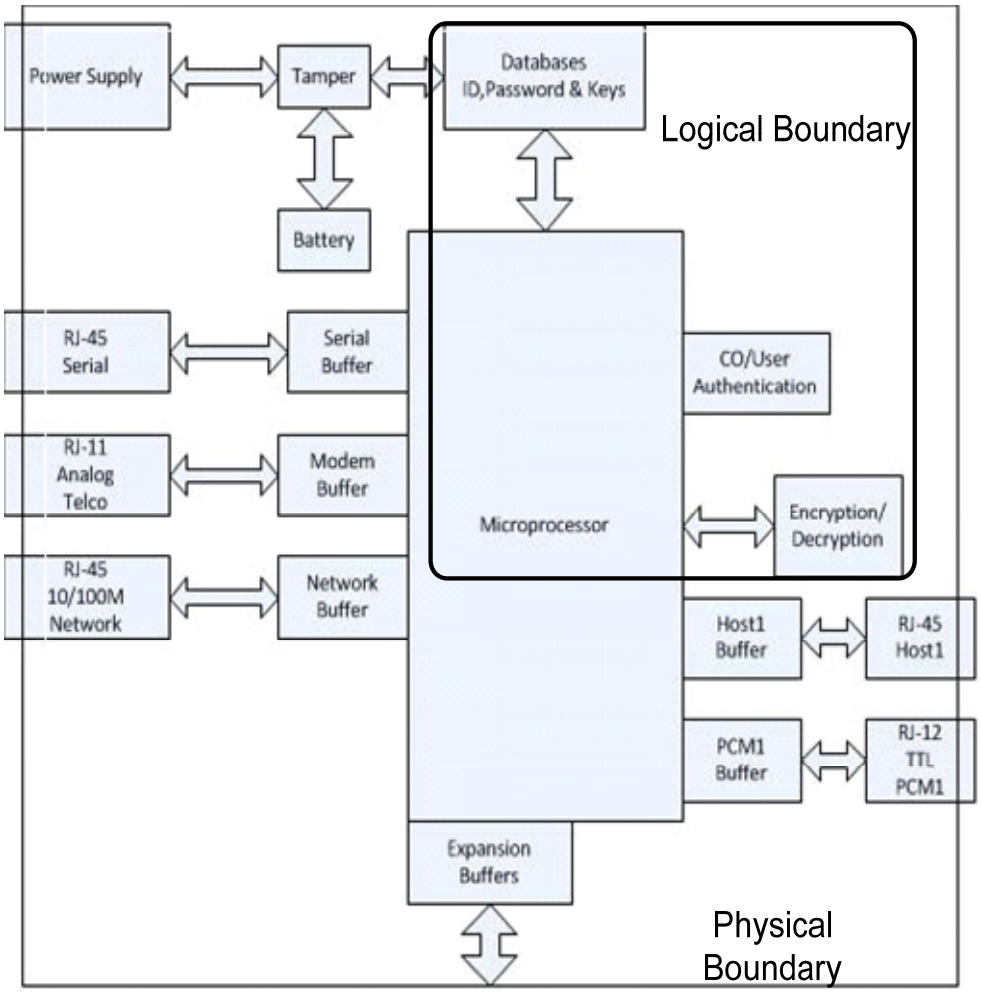


Figure 2-1 Cryptographic Boundary

FIPS Logical Interface	LED	Network Port	Modem Port	Host Port	PCM Port	Serial Console Port	Reset Switch	Tamper Switch
Data Input Interface		X	X	X				
Data Output Interface		X	X	X	X			
Control Input Interface		X	X			X	X	X
Status Output Interface	X							

Table 2-1 Logical Interfaces

2.1 Flash Memory

The flash memory contains the firmware code to run the Port Authority. At power up, the code will be loaded in the DRAM.

2.2 Dynamic Memory DRAM

The DRAM is where the code runs during the Port Authority is on. At power up, after the code is loaded, the code is tested, before running, for integrity using a HMAC function.

2.3 Real Time Clock RTC

The RTC keeps the time even for the power is off by using the battery backup. It used for the logging and the RNG computations.

2.4 Static Memory SRAM

The SRAM, with battery backup, keeps all the databases including the CSPs.

2.5 Field Programmable Gate Array FPGA

The FPGA contains the AES encryption/decryption engine.

2.6 Tamper Switch

The tamper switch, mounted directly on the PCB, will zero all the CSPs and unit's parameters during a case opening.

2.7 Host Port /RJ-45

The Host Port(s) on a PA connects to serial port of equipment that requires security protections over PSTN, such as Firewalls, Routers, and Switches.
Clear text data moves in/out of Port Authority through each RJ-45 connectors labeled Host. Each Host Port has the following Signals for EIA-232 interface with the RJ-45 cable and DB-25 connector. The signals are DCD, DTR, RTS, CTS, GND, DSR, TxD, and RxD.

2.8 Network Port/RJ-45

The network port connects to 10/100 Mbps Ethernet network. This port can connect between a client and a remote in encryption mode and between network appliances in clear text.

2.9 Modem Port/ RJ-11

Operator authentication 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).

2.10 Serial Console Port

The Console Port is used to program the Port Authority using the Front End Loader, a GUI package. The FEL does not save any data of Port Authority. With FEL the Crypto-Officer will be able to change the system parameters such as the Host port speed, data bits, and parity, synchronize time and date with the PC, edit the Crypto-Officer ID and password, perform firmware upgrades, add/delete/modify Users credential and erase/add cryptographic keys. The Crypto-Officer will be able to review and delete audit trail activity of Users with the FEL application.

2.11 PCM Port

PCM are remote to the Port Authority. These modules are used to re-start (turn off then turn on) the power of remote devices that may have become inoperative. This will reset the device and usually restore operation. PCM 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. PCM are controlled by signals sent from the Port Authority.

The rear panel of the Port Authority contains port(s) labeled Power Control Modules. Each port can control a single remote PCM.
The Port Authority is connected to a PCM via a cable. One end of the cable is inserted into the RJ-11 receptacle (PCM) located on the rear of the Port Authority and the other end of the cable is inserted into the RJ-11 receptacle located on the remote PCM.

2.12 Reset Switch

The reset switch, that be actuated via a small hole in the front panel, will bring the unit to a soft reset if push for more than 3 seconds or a full reset, by zeroed the CSP and unit parameters, if pushed for more than 12 seconds.

2.13 Power

The PA111-SA model uses an external supply providing a 12V DC 15W.
The RM models are directly connected to the AC:

Voltage: 100 to 240 V AC 50/60 Hz
Power: 15 W Max.

2.14 I/O Modules

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

2.15 User Authentication Module

The User Authentication Module will read data from the Modem or Network Buffer to authenticate the operator. If the User ID is correct the User Authentication Module will initiate the Encryption Module. After the Port Authority is in Encrypted mode using a 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 Module for encrypting/decrypting data.

The User ID and keys must be loaded in the Port Authority by the Crypto-Officer prior to an 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.

2.16 Encryption Module

The Encryption Module implements AES algorithms for encryption and decryption of data.

2.17 Databases

The Databases, loaded in the SRAM, contain the following items: port parameters, which include number of data bits, baud rate, serial port flow control; keys, IVs, RNG results and the User's credentials.

2.18 Buffers

The Buffers are circular buffers that hold inputs and output from a port. Buffers are read by the Cryptographic Module to encrypt/decrypt data using an AES algorithm.

3 Physical Security

3.1 Physical Embodiment

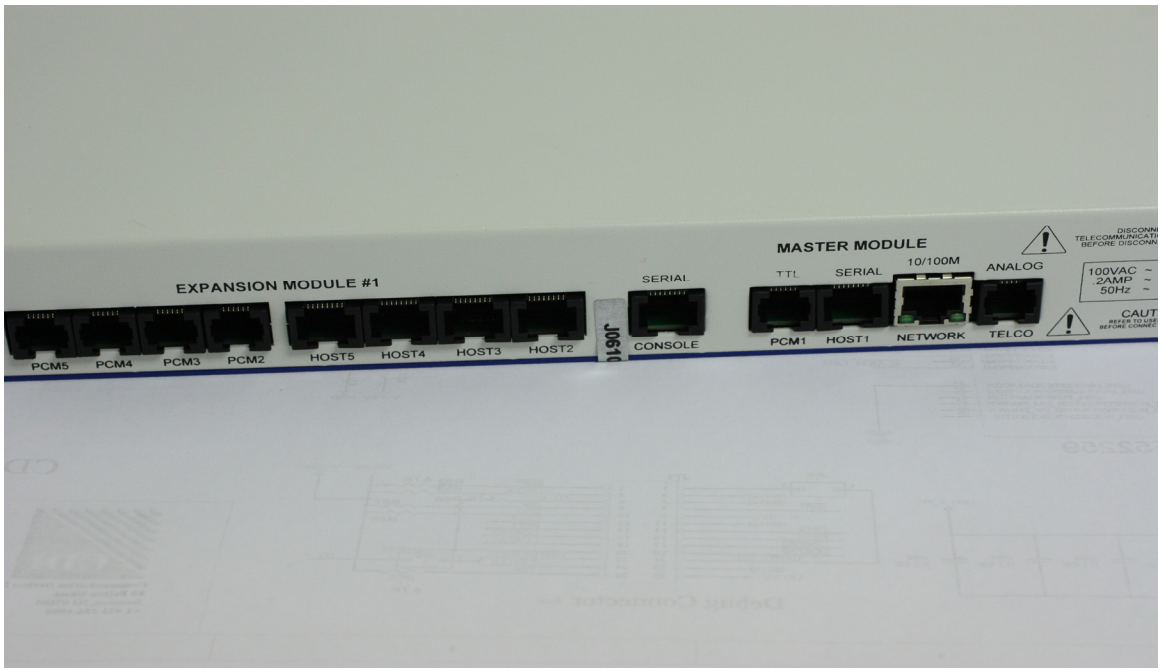
The Port Authority Series module, a multi-chip stand-alone cryptographic module, consists of a number of IC chips mounted on a printed circuit board contained within a protected enclosure. The enclosure contains tamper seals that will destruct if an attempt is made to remove them.

3.1.1 Tamper Seals

The tamper seals are applied on the unit before shipment as following:

- PA111-SA: 2 tamper seals, one on each side.

- PA111-RM/PA155-RM/PA199-RM: 3 tamper seals, one on each side and an additional one on the back.



If any attempt is made to remove or open the top cover tamper seal(s) will be destroyed.

3.1.2 Tamper Switch

The main circuit board contains a tamper switch. The tamper switch will trip if an attempt is made to remove the top cover. The top cover for the PA111-SA (Stand Alone), PA111-RM (Rack Mounted), PA155-RM and PA199-RM must be removed in order to access the chassis base and Printed Circuit Board(s).

If the tamper switch is tripped, the SRAM containing the unit parameters, audit trail, all keys and User information will be zeroed. The zeroization circuit will activate regardless if the SRAM is powered by battery backup or powered by AC. All Integrated Circuit chips are standard industrial IC.

3.2 Enclosure

The enclosure consists of a bottom chassis with front bezel and a Top Cover with back panel.

3.2.1 PA111-SA Stand Alone Chassis

The PA111 enclosure is 5.3 inches (135 mm) wide, 6.8 inches (173 mm) deep and 1.6 inches (40 mm) height. The cover provides room for the connector cutouts located on the rear of the assembled unit. The cover is inserted into the chassis base with four (4) screws.

3.2.2 PA111-RM, PA155-RM and PA199-RM Rack Mount Chassis

The chassis base mounts in a standard 19 inches rack cases. The enclosure is 16.8 inches (427 mm) wide by 6.8 inches (173 mm) deep and 1.6 inches (40 mm) height. The cover is inserted into the chassis base with four (4) screws on the side and three (3) screws on the top.

4 Roles and Services

The services available to a Crypto-Officer Role and User Role are as follows:

Service	Crypto-Officer Role	User Role
Encryption/Decryption	Yes	Yes
Message Integrity	Yes	Yes
Audit Log	Yes	No
Module Management	Yes	No
Key Exchange	Yes	Yes
Firmware Load	Yes	No
Reset[1]	Yes	Yes
Self Tests[2]	Yes	Yes

Table 4-1 Services Authorized for Roles

Note[1]: A person who has physical access to the Port Authority can press the Reset button to reset the module.
Note[2]: A person who has physical access to the Port Authority can power cycle the module to initiate the Self Tests.

4.1 Crypto-Officer Role

When receiving or programming a unit the following steps need to be followed to assure the module integrity:

1. Check if the tamper seals are intact and no physical sign of intrusion is visible.
2. After power-up and initialization, the alarm LED (ALM) must stay extinguished.

In case of no compliance, the unit must be returned immediately to the factory.
Note: In case the alarm LED is illuminated, the module is disabled.

The Port Authority unit supports only one Crypto-Officer for the purpose of programming the user and parameters. 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 Serial Console on the Port Authority. This is the only port that can be used to program and/or modify the Port Authority when connected directly to a computer.

With Front End Loader the Crypto-Officer will be able to change the system parameters such as the Host port speed, data bits, parity, synchronize 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, save and delete audit trail activity of Users with the Front End Loader program.

4.2 User Role

When using a unit the following steps need to be followed to maintain the module integrity:

1. Check if the tamper seals are intact and no physical sign of intrusion is visible.
2. After power-up and initialization, the alarm LED (ALM) must stay extinguished.

In case of no compliance, the unit must be returned immediately to the factory.

Users have access to the serial port (Host 1) to communicate in an encrypted mode to a remote unit. To gain access to a Remote Host, PCM and Network port, the User must first authenticate himself and Port Authority must enter encryption mode. Once he has authenticated he will be granted access to a remote port, power port or the network 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 databases.

4.3 Services

4.3.1 Cryptographic Operations

4.3.2 Encryption

Port Authority will encrypt the data using an AES algorithm before sending it out to the Modem or Network port. The purpose is to secure the data to protect against unauthorized viewing and/or use.

4.3.3 Decryption

Port Authority will decrypt data using an AES algorithm that it receives from the client and deliver the data to the equipment connected to the remote unit. 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 appliance.

4.3.4 No Security/Bypass

No Security/Bypass is a non-FIPS mode. Port Authority, when programmed as No Security/Bypass mode, can send and receive clear text data. The purpose of this mode is when security of data is not needed. This occurs when security is disabled in the unit by the Crypto-Officer and all the CSPs are deleted. In this case the unit will be running in a non-FIPS mode and the SEC LED will stay extinguished.

4.3.5 Message Integrity

Port Authority uses the HMAC function.

4.3.6 Key Management

Using AES Key Wrapper protects against attack of the ephemeral key exchange. The Key exchange is protected using a HMAC function.

4.3.7 Reset

A manual reset, by pressing the reset switch over 12 seconds, will result to a zeroization of the CSPs.

4.3.8 Firmware Load

Port Authority allows a Crypto-Officer to update the firmware in the devices.

4.4 Access Control

Table 4.4-1 Critical Security Parameter (CSP), below, shows the Critical Security Parameters that are stored in the Port Authority's tamper protected SRAM and the roles that have access to them:

Service	Key or/CSP	Access (R/W/E)
Encryption/Decryption	Secret Key[1]	Crypto-Officer Role (W/E)
		User Role (E)
	Session Key[2]	Crypto-Officer Role (E)
		User Role (E)
Message Integrity	Secret Key[1]	Crypto-Officer Role (W/E)
Module Management[5]	User ID	Crypto-Officer Role (RW/E)
		User Role (E)
	Password	Crypto-Officer Role (W/E)
		User Role (E)
	Secret Key[1]	Crypto-Officer Role (R/W)
	RNG Seed Key[3]	Crypto-Officer Role (R/W)
	RNG Seed	Crypto-Officer Role (E)
Key Exchange	Secret Key[1]	Crypto-Officer Role (E)
		User Role (E)
	Session Key[2]	Crypto-Officer Role (E)
		User Role (E)
Reset	CSPs Zeroization	Crypto-Officer Role (E)
		User Role (E)
Self Tests	Integrity Key[4]	User Role (E)

Table 4.4-1 Critical Security Parameter (CSP)

Note[1]: The Secret Key is an AES key used to transmit the Session Key via AES key wrapping. This key is entered manually into the Port Authority during module configuration.

Note[2]: The Session Key is an AES key generated by the Port Authority (remote unit) using the ANSI X9.31 Appendix A.2.4 RNG.

Note[3]: The RNG Seed Key is a key manually entered into the Port Authority during module configuration.

Note[4]: The Integrity Key is a hardcoded HMAC key embedded in the Port Authority for firmware integrity check.

Note[5]: The Module Management service zeroizes the Port Authority when the module transits into the non-FIPS mode.

4.5 Module Management

The Port Authority permits the editing by the authenticated Crypto-Officer of the following:

1. Network properties
2. Serial port properties
3. Host ports properties
4. Modem port properties

4.6 Audit Log

The Port Authority saves up to 150 transactions for review by the Crypto-Officer with the Front End Loader.

4.7 Operator Authentication

The Port Authority by default will not authenticate and or operate until the unit has been programmed with operators, keys and system parameters. If an external operator dials into the Port Authority with a remote FIPS 140-2 validated PA, 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.

The Crypto-Officer gains access to program a Port Authority only via the Front End Loader.

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.

4.8 Identity Based Authentication

The Port Authority provides identity-based authentication. Users do not have access until a valid ID and Password are entered. The module will only echo '*' for each character of password. The User ID and password each has a minimum of 4 printable characters. The chance that a random attempt will be accepted is less than 1 in 1,000,000; every graphic ASCII character can be used ((95^4) = 81,450,625). After 3 failed attempts the call will be dropped and require re-dialing. At most 30 logins can be attempted in 1 minute; therefore, multiple attempts in 1 minute have a probability less than 1 in 100,000.

4.9 Types of Users

The term User refers to a person using the device.

4.9.1 Encryption User

An Encryption User has either a Crypto-Officer role or a User role. The Encryption User uses the encryption/decryption services of the Port Authority and the communication between the Port Authorities is fully protected by encryption. When the Port Authority is

operated in FIPS mode, a new user will be assigned a role, User ID and password by the Crypto Officer. The User ID will be sent in the clear while the password will be sent encrypted via an AES algorithm.

An example of Challenge/Response with complete session encryption involves a User that is prompted (Challenge) for its User ID and 4 to 10-character password. The User enters the information (Response) and attempts to log into a remote Port Authority. Once the User has sent the User ID in the clear, the Port Authority generates a unique session key. The module looks up the Client's encryption key based on the ID entered. The session key is sent encrypted AES Key wrapper to the Client using that encryption key. If the Client uses the same secret key, the session key can be properly 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 an AES algorithm and the User gains access to the appliances connected to the remote unit.

4.9.2 User without Encryption

When the Port Authority is programmed to run in the non-FIPS (No Security/Bypass) mode, all the sessions are not encrypted and no CSPs are stored in the unit. Any user of the Port Authority is a User without Encryption.

5 Operational Environment

The Port Authority uses a limited operational environment. The code that is executed in the Port Authority does employ a RTOS 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.

5.1 PA-111-SA/RM

The Port Authority-111, mostly uses as a client, is a secure port that allows access via dial up modem and Network to communicate with remote PA. The remote device can regulate network appliances with serial control signals, network and Power Control Module (PCM).

5.2 PA-155-RM

The Port Authority-155, mostly use as remote, is a secure port switch that allows a client to access up to 5 remote devices, a Network port and also control signals up to 5 Power Control Modules (PCM).

5.3 PA-199-RM

The Port Authority-199, mostly use as remote, is a secure port switch that allows a client to access up to 9 remote devices, a Network port and also control signals up to 9 Power Control Modules (PCM).

Use of the cryptographic module is limited to two Users at a time.

The Port Authority only provides for 2 Users connection at a time, one with the modem and the other with the network. A User must authenticate to gain access to the Cryptographic Module. Only the data that flows to and from the Port Authority uses the Cryptographic Module. Any other User attempting to dial in to the Port Authority will receive a busy signal

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 using the dialup modem.

By the statement above it is impossible to have multiple operators connected to the Port Authority at the same time using Network, since only one Telnet can be programmed.

6 Key Management

Keys/CSPs	Storage Location	Storage Method	Input Method	Output Method	Zeroization
Secret Key[1]	SRAM	Plaintext	Manual	None	Tampering / Reset
Session Key[2]	RAM	Plaintext	Generated internally	None	Session termination
RNG Seed Key	SRAM	Plaintext	Manual	None	Tampering / Reset
ID	SRAM	Plaintext	Manual	None	Tampering / Reset
Password	SRAM	Plaintext	Manual	None	Tampering / Reset

Table 6 Module Keys and CSPs

Note[1]: The Secret Key is an AES key shared between a Client Port Authority and a Remote Port Authority. It is used to transmit the Session Key via AES Key wrapping. This key is entered manually into the Port Authority during module configuration

Note[2]: The Session Key is an AES key.

Key and Parameter entry – All keys, IDs, passwords and system parameters with the exception of the Firmware Integrity key and Session keys can be entered into Port Authority through the Front End Loader in clear text when locally connected.

Key output – Only the session key wrapped with the secret key is outputted. Review of the keys that have been entered is not possible.

Key zeroization – When the unit is physically opened up, there is a tamper switch that will cause a short across SRAM power inputs and disconnect the unit power supply, which in turn will zero out, reset the SRAM including keys, Crypto-Officer ID, User ID, passwords, log and the unit parameters. During a loss of power, the SRAM is battery backed up to save the keys and User data stored within SRAM. Only the Integrity key that is hard-coded into the firmware would not be zeroed out. All the keys will be destroyed by overwriting the firmware.

Key generation – The key generation process for creating the Seed and Session keys adheres to the ANSI X9.31 Appendix A.2.4 Pseudo-Random Number Generator.

6.1 Key Storage

Keys, in clear text, are stored packed BCD format in the Port Authority's battery backup SRAM. If power is lost to SRAM and the battery is low, the keys will be zeroed out. The SRAM power circuitry includes a tamper switch located behind the cover panel. If the switch is tripped by removing the cover, 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 SRAM. Each AES key requires 16, 24 or 32 bytes of SRAM following the encryption strength.

The Crypto Officer is required to enter a RNG seed key when the Port Authority is configured to run in FIPS mode.

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 units are generated by the Port Authority. The key generation process for creating the keys uses ANSI X9.31 Appendix A.2.4 Pseudo-Random Number Generator to create the ephemeral keys and IVs. The keys are distributed by using AES key wrapper management.

6.2 Key Archiving

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

7 Cryptographic Algorithms

The cryptographic algorithms used in the Port Authority are the following:

1. AES (Cert. #1375) ECB(e/d;128, 192, 256); CBC (e/d; 128, 192, 256); CFB8(e/d;128, 192, 256)
2. SHS (Cert. #1257) SHA-1 (BYTE-only)
3. HMAC (Cert. #808) HMAC-SHA1
4. RNG (Cert. #758) ANSI X9.31 [AES-128Key AES-192Key AES-256Key]

8 FCC Approval

Port Authority PA111, PA155 and PA199 are FCC approved for Part 15 Class A.

9 Self Tests

The self-tests are run every time Port Authority is powered up in crypto mode 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:

9.1 Power-Up Tests

- Firmware Integrity - HMAC-SHA-1 Calculation Test
- HMAC-SHA-1 Known Answer Test
- AES Known Answer Test
- Random Number Generator Known Answer Test

9.2 Conditional Tests

- Bypass Test
- Manual Key Entry Test
- Firmware Load HMAC-SHA-1 Calculation Test
- Continuous Random Number Generator Test

10 Design Assurance

10.1 Engineering Design Review (EDR)

The EDR provides a formal in-depth review of a project with the engineering design staff and external expertise.

10.2 Process Verification

The process verification is actively performed for every phase of the project to keep the project on track.

10.3 Update Risk Analysis (URA)

The URA evaluates the risks and checks preventive measures necessary to negate or reduce the risks during the project life.

11 Security Policy Rules Of Operation

Port Authority is designed to meet FIPS 140 overall Level 2 requirements after being locally programmed via the FEL by a Crypto-Officer.

11.1 Port Authority Programming steps

1. Power up the unit
2. Start FEL configuration Setup
3. Specify the Connection Properties; Com Port Selection and Baud Rate.
4. Enter in Device System Parameter
5. Choose Device Mode to "Enable Security"
6. Enter device name, AES key size and seed for RNG
7. Verify RNG seed by entering the seed a second time; if the module accepts the key, the module's SEC LED (RED) will be illuminated and the module is in FIPS mode.
8. Enter Crypto-Officer credentials
9. Enter Client ID(s) and key(s) and verify the key by entering the key a second time
10. Enter users credentials for the remote units

11.2 User Access

To gain access to the host device (Remote) that Port Authority (Client) is protecting, the Port Authority must be in a cryptographic mode (FIPS mode) such that all data in/out of the modem or network to the PTSN is encrypted via an AES algorithm. The User must be programmed in the database to have the rights to the host port of Port Authority. Each User first has to be authenticated before Port Authority transfers encrypted data.

11.3 Access Notes

A host Port Authority will only authenticate in the cryptographic mode (FIPS) with a client that has the same 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 when locally programmed.

All data in/out of Port Authority for programming User ID's, Keys, Port Parameters, and Device Options will be encrypted when remotely programmed.

The firmware can be updated in the Port Authority by over writing the existing FIPS 140 validated firmware with a new version of FIPS 140 Validated firmware. The update uses ANSI X9.31 - HMAC Calculation Test when updating the firmware.

CDI does not have any databases or backdoor access to customer data.

All cryptographic circuit and customer database are protected by a tamper switch and tamper evident seals to detect any physical tampering.

A power-up or a power cycle will initiate a series of self-tests without any user involvement.

Any self-test failure will put the module in an error state and block any module function. Only full authorization will permit user to access a module service