Communication Devices Inc.

Port Authority Series

FIPS 140-3 Non-Proprietary Security Policy

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

This document is copyright © Communication Devices, Inc. 2026

Document Version: 2.0

Date: 1/8/2026

Table of Contents

1 General 6
1.1 Overview 6
1.2 Security Levels 6
2 Cryptographic Module Specification 6
2.1 Description 6
2.2 Tested and Vendor Affirmed Module Version and Identification 13
2.3 Excluded Components 14
2.4 Modes of Operation 14
2.5 Algorithms 15
2.6 Security Function Implementations 17
2.7 Algorithm Specific Information 19
2.8 RBG and Entropy 19
2.9 Key Generation 20
2.10 Key Establishment 20
2.11 Industry Protocols 20
2.12 Additional Information 21
3 Cryptographic Module Interfaces 21
3.1 Ports and Interfaces 21
3.2 Control Interface Not Inhibited 22
4 Roles, Services, and Authentication 22
4.1 Authentication Methods 22
4.2 Roles 23
4.3 Approved Services 24
4.4 Non-Approved Services 31
4.5 External Software/Firmware Loaded 31
4.6 Bypass Actions and Status 32
5 Software/Firmware Security 32
5.1 Integrity Techniques 32
5.2 Initiate on Demand 32
6 Operational Environment 32
6.1 Operational Environment Type and Requirements 32
6.2 Configuration Settings and Restrictions 32
7 Physical Security 32
7.1 Mechanisms and Actions Required 33
7.2 User Placed Tamper Seals 33

8 Non-Invasive Security 35
9 Sensitive Security Parameters Management 35
9.1 Storage Areas 35
9.2 SSP Input-Output Methods 35
9.3 SSP Zeroization Methods 36
9.4 SSPs 37
10 Self-Tests 42
10.1 Pre-Operational Self-Tests 42
10.2 Conditional Self-Tests 43
10.3 Periodic Self-Test Information 44
10.4 Error States 46
11 Life-Cycle Assurance 46
11.1 Installation, Initialization, and Startup Procedures 46
11.2 Administrator Guidance 46
11.3 Non-Administrator Guidance 47
11.4 End of Life 47
12 Mitigation of Other Attacks 47

List of Tables

Table 1: Security Levels 6
Table 2: Tested Module Identification – Hardware 13
Table 3: Modes List and Description 14
Table 4: Approved Algorithms 16
Table 5: Non-Approved, Allowed Algorithms with No Security Claimed 16
Table 6: Security Function Implementations 19
Table 7: Entropy Certificates 19
Table 8: Entropy Sources 19
Table 9: Ports and Interfaces 21
Table 10: Authentication Methods 22
Table 11: Roles 23
Table 12: Approved Services 31
Table 13: Mechanisms and Actions Required 33
Table 14: Storage Areas 35
Table 15: SSP Input-Output Methods 36
Table 16: SSP Zeroization Methods 36
Table 17: SSP Table 1 39
Table 18: SSP Table 2 42
Table 19: Pre-Operational Self-Tests 42
Table 20: Conditional Self-Tests 44
Table 21: Pre-Operational Periodic Information 45
Table 22: Conditional Periodic Information 45
Table 23: Error States 46

List of Figures

Figure 1: Block Diagram Depicting the Cryptographic Boundary 8
Figure 2: PA111-SA and PA111-RM Hardware Diagram 8
Figure 3: PA121 Hardware Diagram 9
Figure 4: PA155 Hardware Diagram 10
Figure 5: PA199 Hardware Diagram 11
Figure 6: PA111-SA 12
Figure 7: PA111-RM 12
Figure 8: PA121-RM 12
Figure 9: PA155-RM 13
Figure 10: PA199-RM 13
Figure 11: PA111-SA Tamper Seal at Side/Bottom 34
Figure 12: PA111-SA Tamper Seal at Side/Bottom 34
Figure 13: PA121-RM Tamper Seals at Side/Bottom and Front/Bottom 34
Figure 14: PA121-RM Tamper Seals at Side/Bottom and Rear/Top 34
Figure 15: PA111-RM, PA155-RM, PA199-RM Tamper Seals at front/Top and Side/Bottom 34
Figure 16: PA111-RM, PA155-RM, PA199-RM Tamper Seals at Rear/Bottom 35

1 General

1.1 Overview

This document sets forth to describe the security rules under which the Port Authority Series cryptographic module (the “module”) will operate, using the terminology contained in the Federal Information Processing Standards Publication 140-3, which is available at https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf on the NIST website. The format of this document follows the requirements specified in NIST SP 800-140Br1.

This non-proprietary security policy may be reproduced or distributed in its entirety, without revision and with copyright notices.

1.2 Security Levels

Section	Title	Security Level
1	General	2
2	Cryptographic module specification	2
3	Cryptographic module interfaces	2
4	Roles, services, and authentication	2
5	Software/Firmware security	2
6	Operational environment	N/A
7	Physical security	2
8	Non-invasive security	N/A
9	Sensitive security parameter management	2
10	Self-tests	2
11	Life-cycle assurance	2
12	Mitigation of other attacks	N/A
	Overall Level	2

Table 1: Security Levels

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

Out of Band Management, or OBM, refers to products that permit secured technician access to "management elements" (e.g. Firewalls, Routers, Bridges, SONET, Switches, Servers, etc.) via dial up telephone lines, isolated cellular networks and other communication channels not in bandwidth of the primary network. As in-band, or part of the primary network, control channels both rely on connectivity in the primary network, they can become useless if there is a failure in primary network. In-band control channels are also subject to interception and other compromised conditions that the primary network could be experiencing. When the primary network goes down or is severely disrupted, control traffic has no way to get between the managed elements and the management workstations. Quite often when a managed element goes down, it loses its network connection, which renders in-band management useless. This is

where the Port Authority cryptographic module always works flawlessly for OBM. To augment the Port Authority usefulness, access via local networks is available.

The module is designed primarily to enable remote access to a device's console port and provide the capability to remotely power the device on or off. The module can address the limitations of network-dependent remote authentication, which can fail if the network is not operational. The module stores its own database of user rights on board or establish a cryptographic Chain-of-Trust, allowing it to operate even in situations where the primary network is inaccessible.

The module supports:

- Dialup speed up to 115.2 Kbps via an internal V.92 modem
- Cellular speed up to 1Mbps via an internal cellular modem
- Network link speed at 1G or 100M
- Power cycling of managed devices via Power Control Module ports (PCM ports)
- Access to managed device's physical console ports via Host ports

The module utilizes TLSv1.3 with AES128-GCM-SHA256 or AES256-GCM-SHA384 cipher suites to safeguard both User-Module and Crypto-Officer-Module connections. For instance, an operator can establish a secure TLS connection to another module located at a remote site, enabling the operator to securely manage devices at that remote site through TLS connection.

Module Type: Hardware

Module Embodiment: Multi-Chip Standalone

Module Characteristics:

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, cellular modem, a Power Control port, a Network port, RJ45 or USB Host 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. The block diagram is depicted in figures below:

Tested Operational Environment's Physical Perimeter (TOEPP):

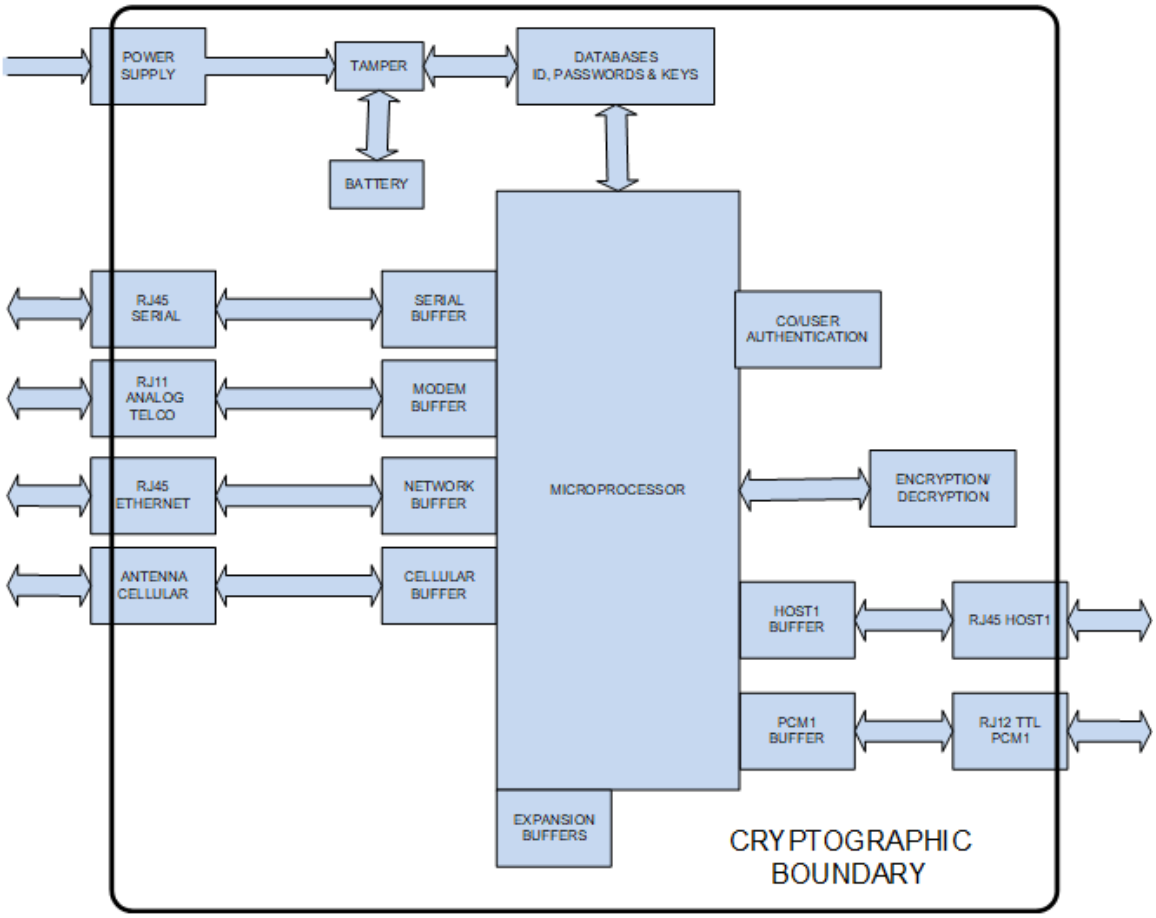

Figure 1: Block Diagram Depicting the Cryptographic Boundary

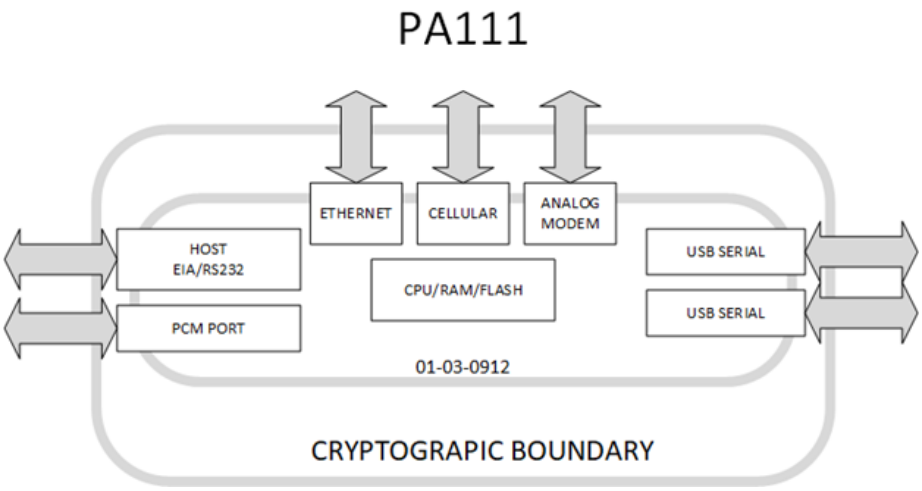

Figure 2: PA111-SA and PA111-RM Hardware Diagram

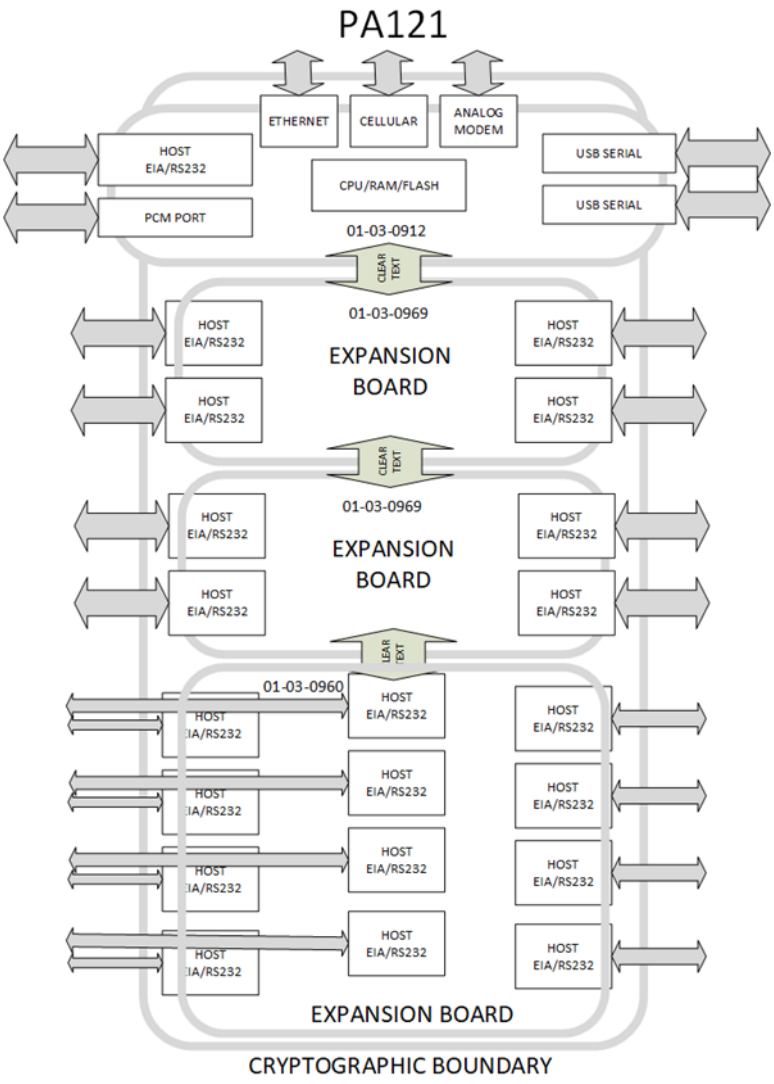

Figure 3: PA121 Hardware Diagram

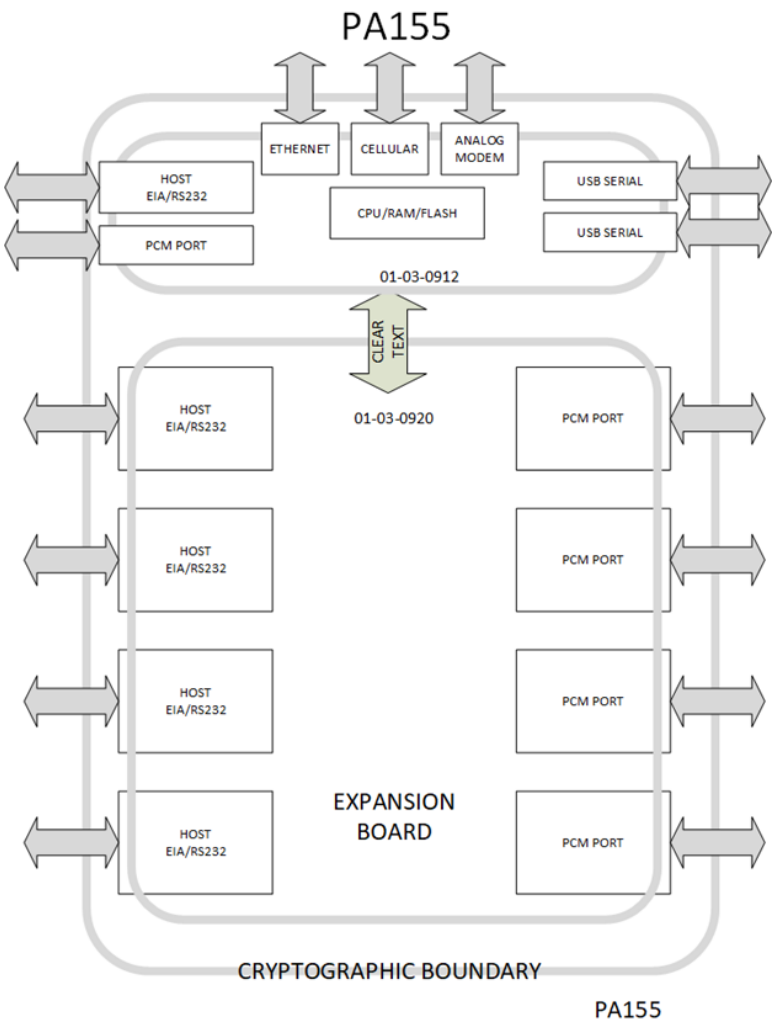

Figure 4: PA155 Hardware Diagram

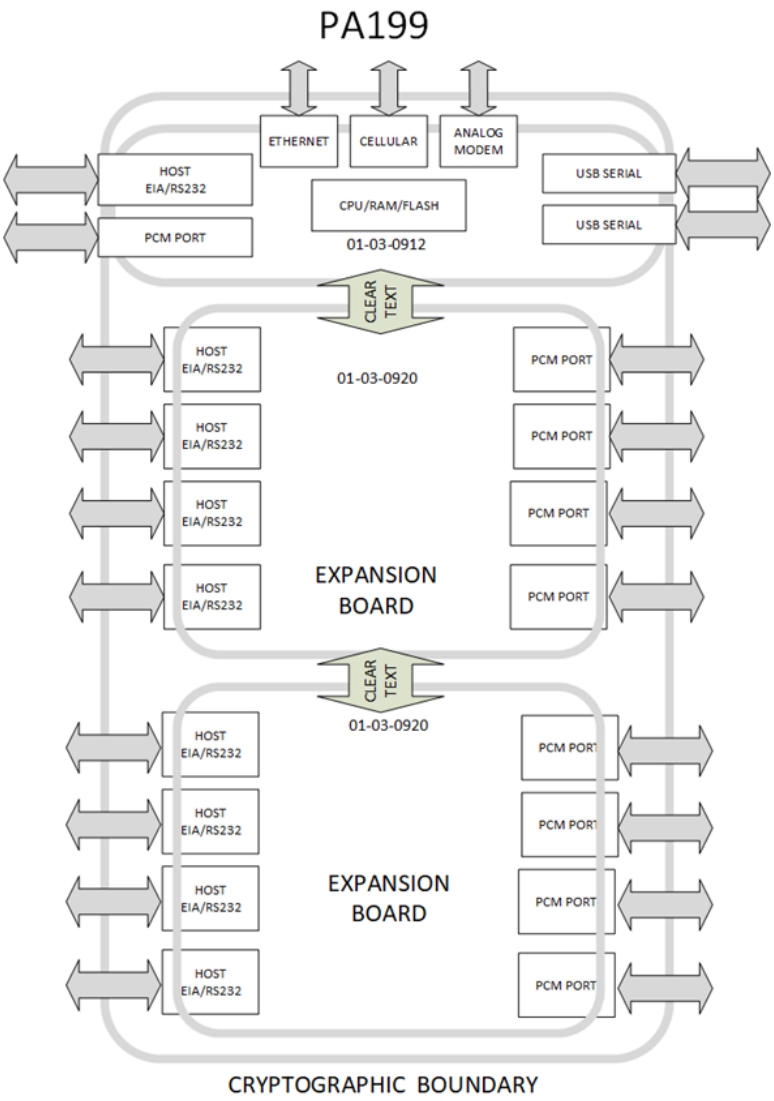

Figure 5: PA199 Hardware Diagram

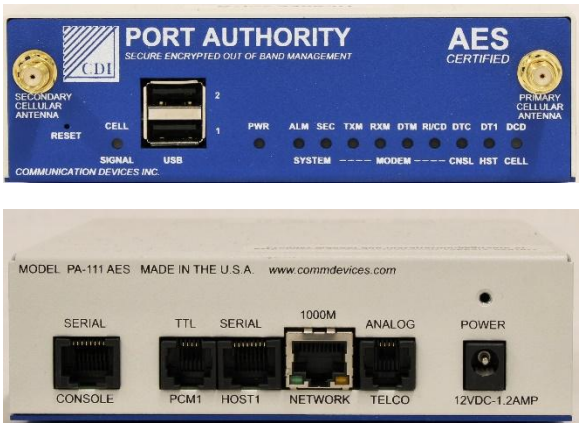

Figure 6: PA111-SA

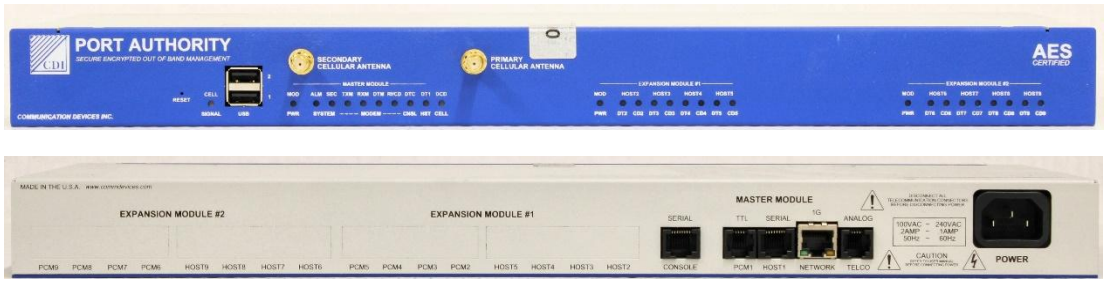

Figure 7: PA111-RM

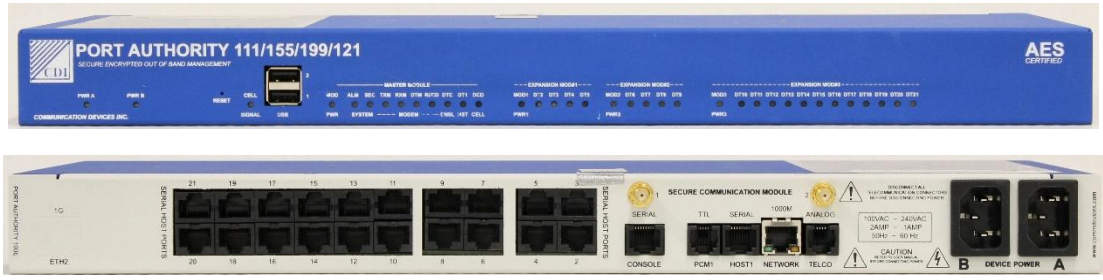

Figure 8: PA121-RM

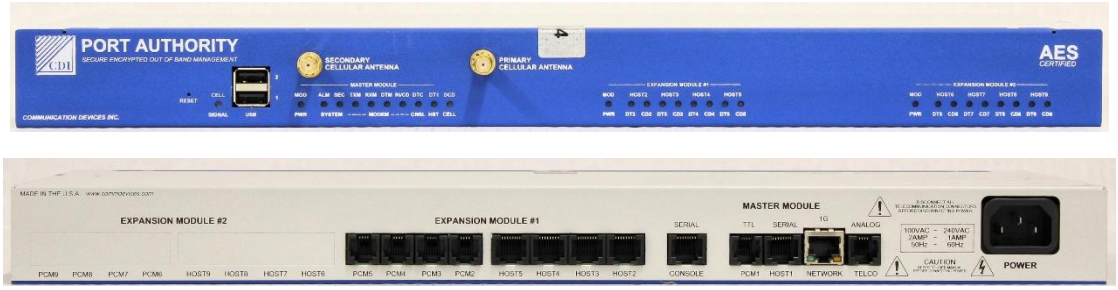

Figure 9: PA155-RM

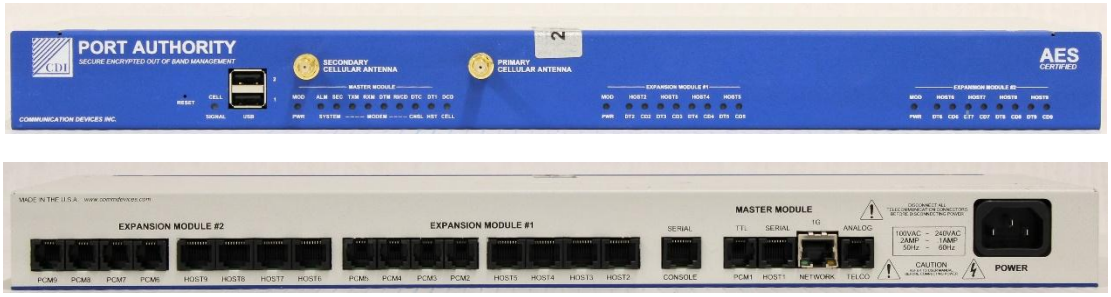

Figure 10: PA199-RM

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

The module operates in a limited operational environment. The module has been tested on the following operating environments:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
PA111-SA	CDI 01-03-0912l	1.0.0	i.MX6 Ultralite (NXP, IMX6, ARM32)	N/A
PA111-RM	CDI 01-03-0912l	1.0.0	i.MX6 Ultralite (NXP, IMX6, ARM32)	N/A
PA121-RM	CDI 01-03-0912l	1.0.0	i.MX6 Ultralite (NXP, IMX6, ARM32)	3 expansion boards (20 serial host ports)
PA155-RM	CDI 01-03-0912l	1.0.0	i.MX6 Ultralite (NXP, IMX6, ARM32)	1 expansion board (4 serial host ports and 4 PCM ports)
PA199-RM	CDI 01-03-0912l	1.0.0	i.MX6 Ultralite (NXP, IMX6, ARM32)	2 expansion boards (8 serial host ports and 8 PCM ports)

Table 2: Tested Module Identification – Hardware

Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets):

N/A for this module.

Tested Module Identification – Hybrid Disjoint Hardware:

N/A for this module.

Tested Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

2.3 Excluded Components

There are no excluded components for this cryptographic module.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved mode	The FIPS 140-3 approved mode of operation (the module supports the Approved mode)	Approved	SEC LED on

Table 3: Modes List and Description

When the module starts up successfully, after passing all the pre-operational self-tests, the module uses the approved mode and all communication is based on authenticated and encrypted access. The device authenticates itself via a certificate issued by a Certificate Authority (CA), allowing clients, possibly other Port Authorities, to verify the authentication of the device.

Operators can be authenticated by credential or via being issued a certificate with permissions embedded within. Certificates are verified by checking the presented certificate against securely stored Certification Authority (CA) Certificates. Each of the authentication methods results in the issuance of a session token that gives access to a REST API that controls all public functions of the device. Login, token issuance and finally API usage are all secured by TLSv1.3.

More detail can be found in section 11.1 and 11.2 Startup Procedures and Administrator Guidance.

Mode Change Instructions and Status:

This is not applicable to this module which implements only one mode of operation, the approved mode of operation.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-GCM	A4440	Direction - Decrypt, Encrypt IV Generation - External Key Length - 128, 256 Tag Length - 128 IV Length - IV Length: 8-1024 Increment 8 Payload Length - Payload Length: 0-65536 Increment 8 AAD Length - AAD Length: 0-65536 Increment 8	SP 800-38D
ECDSA KeyGen (FIPS186-4)	A4440	Curve - P-256 Secret Generation Mode - Extra Bits	FIPS 186-4
ECDSA KeyVer (FIPS186-4)	A4440	Curve - P-256	FIPS 186-4
ECDSA SigGen (FIPS186-4)	A4440	Component - No Curve - P-256 Hash Algorithm - SHA2-256	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A4440	Component - No Curve - P-256 Hash Algorithm - SHA2-256	FIPS 186-4
HMAC DRBG	A4440	Prediction Resistance - No Supports Reseed - Yes Mode - SHA2-256 Entropy Input - Entropy Input: 256 Nonce - Nonce: 128 Personalization String Length - Personalization String Length: 0 Additional Input - Additional Input: 0 Returned Bits - 256	SP 800-90A Rev. 1
HMAC-SHA2-256	A4440	MAC - MAC: 32-256 Key Length - Key Length: 256-512 Increment 8	FIPS 198-1
HMAC-SHA2-384	A4440	MAC - MAC: 32-384 Key Length - Key Length: 256-512 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A4440	Domain Parameter Generation Methods - P-256 Hash Function Z - SHA2-256 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3

Algorithm	CAVP Cert	Properties	Reference
SHA2-256	A4440	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-384	A4440	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA3-256	A3214	Message Length - Message Length: 0-65536 Increment 8	FIPS 202
TLS v1.3 KDF (CVL)	A4440	HMAC Algorithm - SHA2-256, SHA2-384 KDF Running Modes - DHE, PSK, PSK-DHE	SP 800-135 Rev. 1

Table 4: Approved Algorithms

The table above lists the approved security functions (or cryptographic algorithms) of the module, including specific key lengths employed for approved services, and implemented modes or methods of operation of the algorithms.

No parts of the TLS 1.3 protocol, other than the approved cryptographic algorithms and the KDF, have been tested by the CAVP and CMVP.

HMAC-SHA-1 and SHA-1 are CAVP tested but not used by the module. AES-ECB is CAVP tested as a prerequisite for AES-GCM but not used by the module.

Vendor-Affirmed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

Name	Caveat	Use and Function
AES-CFB8	Payload is obfuscated and considered equivalent to plaintext	SNMPv3 payload
SNMP	Keys derived using the no-security claimed key localization function	SNMPv3 key derivation

Table 5: Non-Approved, Allowed Algorithms with No Security Claimed

The module implements the SNMPv3 protocol which does not conformed to RFC 2574 which mandates the use of the HMAC-SHA-96 authentication protocol and CBC-DES symmetric encryption protocol. The module SNMPv3 protocol uses the HMAC-SHA2-256 and AES-CFB8 instead. Data transmitted over the SNMP protocol only contains network metrics data that is non-sensitive and is considered plaintext.

Non-Approved, Not Allowed Algorithms:

N/A for this module.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
TLS Key Agreement	KAS-Full	SP 800-56Arev3 key establishment + TLS v1.3 KDF	Scheme:ephemeralUnified Reference:IG D.F Scenario 2, path (1), no key confirmation, key derivation using TLSv1.3 KDF (RFC 8446) mapping to NIST SP 800-133rev2 (Section 6.3 Option #3), SP 800-56Crev2, and SP 800-108 Caveat:Key establishment methodology provides 128 bits of encryption strength	KAS-ECC-SSC Sp800-56Ar3: (A4440) TLS v1.3 KDF: (A4440) HMAC DRBG: (A4440) SHA2-256: (A4440) SHA2-384: (A4440) HMAC-SHA2-256: (A4440) HMAC-SHA2-384: (A4440)
TLS Payload Encryption	BC-Auth	Data encryption and integrity of TLS v1.3 protocol payload		AES-GCM: (A4440)
TLS KTS	KTS-Wrap	CSP through the TLS v1.3 protocol payload	Reference:IG D.G, Additional Comment 8, approved key transport method) Caveat:Key transport provides 128 bits of encryption strength	AES-GCM: (A4440)
TLS Server Authentication	DigSig-SigGen	Signing messages within TLS handshake		ECDSA SigGen (FIPS186-4): (A4440) SHA2-256: (A4440) SHA2-384: (A4440)
HMAC DRBG	DRBG	HMAC DEBG using SHA2-256		HMAC DRBG: (A4440) HMAC-SHA2-256: (A4440)
Certificate Generation	AsymKeyPair-KeyGen	Generate a signing keypair for		ECDSA KeyGen (FIPS186-4):

Name	Type	Description	Properties	Algorithms
	AsymKeyPair-KeyVer	use within TLS		(A4440) ECDSA KeyVer (FIPS186-4): (A4440) ECDSA SigGen (FIPS186-4): (A4440) HMAC DRBG: (A4440)
Certificate Verification	DigSig-SigVer	Verify trust for receiving certificates		ECDSA SigVer (FIPS186-4): (A4440) SHA2-256: (A4440)
SigGen	DigSig-SigGen	Signature generation		ECDSA SigGen (FIPS186-4): (A4440)
Certificate Authentication	DigSig-SigVer	Operator authentication using certificate		ECDSA SigVer (FIPS186-4): (A4440)
Password Authentication	SHA	Operator authentication using password		SHA2-256: (A4440)
Factory Pre-load	DigSig-SigVer	Build server public key for used to verify update package and firmware integrity		ECDSA SigVer (FIPS186-4): (A4440)
Entropy Source	ENT-NP	Entropy source		
Password Hash	SHA	Generate a hashed password		SHA2-256: (A4440)
Module Reset	AsymKeyPair-KeyGen AsymKeyPair-KeyVer	Reset module to factory default		ECDSA KeyGen (FIPS186-4): (A4440) ECDSA SigGen (FIPS186-4): (A4440)

Name	Type	Description	Properties	Algorithms
				ECDSA SigVer (FIPS186-4): (A4440)
SigVer	DigSig-SigVer	Signature verification		ECDSA SigVer (FIPS186-4): (A4440)

Table 6: Security Function Implementations

2.7 Algorithm Specific Information

AES-GCM IV Generation
The module implements the TLS protocol version 1.3 defined in RFC 8446. The module's TLS implementation only uses AES-GCM cipher suites, and the IV is generated and only used within the TLS implementation within the cryptographic boundary of the module. The GCM IV generation complies with IG C.H under scenario 5.

When the IV exhausts the maximum value of $2^{64} - 1$, the module will establish a new encryption key. The output (key, IV) pair collision probability is less than 2^{-32}.

2.8 RBG and Entropy

Cert Number	Vendor Name
E100	Communication Devices Inc.

Table 7: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
CDI CPU Time Jitter Based Non-Physical Entropy Source	Non-Physical	Linux 4.14 on i.MX6 Ultralite (NXP, IMX6, ARM32) processor	8	5.921367	A3214

Table 8: Entropy Sources

Entropy Information:
The module provides the CDI CPU Time Jitter for generation of random numbers with a validated SHA3-256 conditioning component (cert. #A3214). The entropy source has undergone the Entropy Server Validation program, obtaining the following ESV cert. #E100. For more information, the following link can be consulted: https://csrc.nist.gov/projects/cryptographic-module-validation-program/entropy-validations/certificate/100.

DRBG Information
Besides the Entropy Source, the module offers a SP 800-90A compliant HMAC DRBG mechanism with an HMAC SHA2-256 for creation of key components of asymmetric keys, and

random numbers. The DRBG is instantiated, using a seed of 440 bits, with 128 bits of encryption strength.

2.9 Key Generation

For generation of ECDSA key pairs, the module implements approved key generation services compliant with [FIPS 186-4] where the key material is directly obtained from an approved [SP 800-90Arev1] HMAC DRBG. The public and private key pair used in the EC Diffie-Hellman KAS are generated internally. They are compliant with NIST [SP 800-56Arev3].

The symmetric keys used in the TLSv1.3 and SNMPv3 contexts are derived using an approved KDF and this method is compliant with section 6.2 of [SP 800-133rev2].

2.10 Key Establishment

Key Agreement
The module provides EC Diffie-Hellman as shared secret computation method to obtain “shared secrets” values.

The security strength of the preceding algorithms is as follows:

- EC Diffie-Hellman key agreement provides 128 bits of encryption strength.

In addition, the module does support Key Derivation methods, listed below:

- Protocol-Suite Key Derivation: TLS 1.3 KDF and SNMPv3 KDF[1].

Key Transport
The module does not transport secret key or private key. However, the module supports public key input and output in TLS payload.

2.11 Industry Protocols

Note: no parts of the TLS v1.3 and SNMPv3[2] protocols, other than the approved cryptographic algorithms and KDFs, have been tested by the CAVP and CMVP. The following table shows the cipher suites information available for this cryptographic module:

Protocol	Key Exchange	Server/Host Authentication	Cipher		Integrity
TLSv1.3		TLS_ AES_128_GCM_SHA256			
	ECDH	ECDSA	AES-GCM		AES-GCM
		TLS_ AES_256_GCM_SHA384			
	ECDH	ECDSA	AES-GCM		AES-GCM
SNMPv3	N/A	HMAC	AES-CFB8		HMAC

[1] This SNMP KDF is a non-approved algorithm used by the module as a non-security function with no security claimed.
[2] This SNMPv3 protocol implements a KDF using SHA2-256, not SHA-1 as specified in SP 800-135r1. The module can only output network metrics containing only non-sensitive status data obfuscated using AES-CFB8. The status data transmitted over this protocol is considered plaintext. No security is claimed for this protocol.

2.12 Additional Information

The base and primary applications installed at factory contains the Build server public key. When the module receives an update, the operator executes the Firmware Upload service and uses the mentioned public key to validate the package. The verification is done before installation and corresponding integrity self-tests are executed as well.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
Cellular Antennas	Control Input Control Output Status Output	CO traffic
Cellular Antennas	Data Input Data Output	User traffic
Console	Control Input Status Output	CO traffic
Host(s)	Data Input	User traffic from managed device
Host(s)	Data Output	User traffic to managed device
Network	Control Input Control Output Status Output	CO traffic
Network	Data Input Data Output	User traffic
PCM	Control Input	User traffic to Power Control Module
Power	Power	VAC or VDC
Reset Switch	Control Input	Hardware reset signal
USB	Data Input	User traffic from managed device
USB	Data Output	User traffic to managed device
LEDs	Status Output	Device status
Telco	Control Input Control Output Status Output	CO traffic
Telco	Data Input Data Output	User traffic

Table 9: Ports and Interfaces

Note: A module can be used to remotely administer another module.

User Traffic
Port Authority User Traffic associated with Control Output, Data Input and Data Output logical interfaces is defined as traffic meant to access the control interfaces of external devices or toggle those device's power via a PCM. The traffic comes into the device via the FIPS secured mechanism and is then acted upon.

In the case of accessing another device's control interface, this is typically done via the RJ45 or USB Host Ports; however, it may also include using the Network Port to access TCP/IP based control interfaces.

In the case of toggling another device's power, the Port Authority will send a signal via a RJ-11 PCM port that will tell connected PCM modules to toggle the power on or off.

Crypto Officer Traffic
Port Authority Crypto Officer (CO) Traffic is associated with Control Input and Control Output logical interfaces and is defined as traffic meant to configuring and securing the Port Authority device.

3.2 Control Interface Not Inhibited

The control output interface is inhibited when the module is running any self-tests specified in Section 10.

4 Roles, Services, and Authentication

The module includes authentication mechanisms compliant with security level 2 as well as User and Crypto Officer roles. The cryptographic module does support concurrent operators using TLS connections, but it does not support concurrent operators using dialup or cellular connection. The Port Authority does not support bypass capability or maintenance role.

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
Certificate	X509v3 for Crypto Officer and User roles	Certificate Authentication	2^128	8.8x10^-17
Credential	ID and Password for Crypto Officer and User roles	Password Authentication	9^58	4.5x10^-15 over analog or 6.0x10^-14 over cellular

Table 10: Authentication Methods

The Port Authority supports two types of authentication mechanisms, certificate and credential. The authentication strength objectives for the modules are:

- a probability of less than one in 1,000,000 that a single attempt will succeed, and
- a probability of less than one in 100,000 that a random attempt will succeed for multiple attempts during a one-minute period.

Certificate
Either via an existing TLS connection between non-user entities or initiating an TLS connection directly, an operator presents a valid certificate that the operator has been granted as the Crypto Officer or User role. The certificate is checked in the following way:

1. The certificate is checked against loaded certificate authority certificates.

2. The x509v3 extension OID 1.3.6.1.4.1.50769.140.3.1 is checked to determine if the operator is a User:
    a. If the extension is present, then the user's Common Name become the name used by the module and is added to the access token.
    b. If not, check to determine if operator is a Crypto Officer.
3. The x509v3 extension OID 1.3.6.1.4.1.50769.140.3.2.2 is checked to determine if the operator is a Crypto Officer:
    a. If yes, then the admin flag is set for this operator, else not set.
4. The x509v3 extension OID 1.3.6.1.4.1.50769.140.3.2.3 is checked to determine the operator's port permissions (access tag):
    a. These tags are added to the access token.
    b. If omitted, the operator will have no access to ports

This login method relies on ECDSA P-256 and SHA2-256 to secure the certificate. Historically, certificate attacks tend to target the hash function via a collision attack. This type of attack would require 2^{128} hashes to be computed. Even if the attack can leverage precomputation, hash generation is bottlenecked by computation power. The device can only produce a few hundred hashes per second, and even specially designed farms filled with devices meant to only generate hashes can produce Gigahashes per second. If all the hash farms worked together and produced 500 Exahashes second. Putting this all together a single attempt has a $1/(2^{128})$ chance of succeeding and even using all the hashing power the chance of success in a minute would be:

$$\frac{\frac{500x10^{18}hashes}{1\ second}\ x\ \frac{60\ seconds}{1\ minute}}{2^{128}hashes} \cong 8.8x10^{-17}$$

Credential
Either via an existing TLS connection between non-user entities or initiating a TLS connection directly, the user presents credentials that correspond to a record in the device indicating User or Crypto Officer permissions.

The Port Authority provides identity-based authentication. Users do not have access until a valid ID and Password are entered. The User ID and Password each has a minimum of 8 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 ($95^8 = 6.6x10^{15}$). For analog calls, 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, yielding a strength per minute of ($30/95^8$). For cellular calls, each login attempt takes approximately 150ms. This means 400 login attempts per minute, yielding a strength per minute of ($400/95^8$).

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Role	CO	Certificate Credential
User	Role	User	Certificate Credential

Table 11: Roles

The Port Authority unit supports the Crypto Officer and User roles. The module also allows concurrent operators with an associated TLS connection. The table below lists the available roles:

Crypto Officer role
The module supports the Crypto Officer role for the purpose of programming the user and parameters. The Crypto Officer will either connect to the device via two possible methods using a TLSv1.3-based API or with a serial connection and terminal emulator.

The Crypto Officer can either authenticate to the module via credential or certificate. In both situations, a time-limited access token will be issued and used by the operator when making requests to perform configuration and management actions restricted to the Crypto Officer role.

User role
The module supports the User role to access a remote device via the module's Host, PCM, or Network port. To gain access to a module's Host, PCM or Network port, a User must first create a secure TLS connection and authenticate to the module, either using certificate or credential authentication.

Once authenticated, the User will be granted access to use the User Access service of the module. The User needs at minimum a User ID and Password to authenticate to the module. Certificate-based authentication is also possible if the User is set up to use certificate-base authentication by the Crypto Officer.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Login	Operator login	Function returns without error	Login request, Password, Operator Certificate	Login failure, login success and access token generated	TLS Key Agreement TLS Payload Encryption TLS Server Authentication SigGen Certificate Authentication Password Authentication	Crypto Officer - Access Token: W,Z - Password : W,E - Operator Certificate : W,E - CA Certificate : E - AES-GCM Key: G,E - TLS Premaster Secret : G,E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- TLS Master Secret : G,E,Z - EC Diffie-Hellman Private Key: G,E,Z - EC Diffie-Hellman Public Key : G,R,Z - Peer EC Diffie-Hellman Public Key: W,E,Z - ECDSA Private Key: E - ECDSA Public Key Certificate : R - DRBG Key: W,E - DRBG V: W,E - Hashed Password : G,E - ECDSA Self-signed Certificate : R User - Access Token: W,Z - Password : W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Operator Certificate : W,E - CA Certificate : E - AES-GCM Key: G,E - TLS Premaster Secret : G,E,Z - TLS Master Secret : G,E,Z - EC Diffie-Hellman Private Key: G,E,Z - EC Diffie-Hellman Public Key : G,R,Z - Peer EC Diffie-Hellman Public Key: W,E,Z - ECDSA Private Key: E - ECDSA Public Key Certificate : R - DRBG Key: W,E - DRBG V: W,E - Hashed

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Password : G,E - ECDSA Self-signed Certificate : R
User Access	Allow user access to control interfaces and managed elements	Function returns without error	Data to and from managed external device	Plaintext traffic to and from managed external device	TLS Payload Encryption Certificate Verification SigVer	Crypto Officer - AES-GCM Key: E - Access Token: R,W,Z - ECDSA Public Key: E - ECDSA Private Key: E User - AES-GCM Key: E - Access Token: R,W,Z - ECDSA Public Key: E - ECDSA Private Key: E
Audit Log	Download event from the device	Function returns without error	Request for module log	Response containing module log	TLS Payload Encryption	Crypto Officer - AES-GCM Key: E - Access Token: R,W,Z
Certificate Management	Create CSR, upload certificates and CA certificates	Function returns without error	Request to get a device's CSR, set devices's certificate,	Response containing a CSR or the status of the set action	TLS Payload Encryption HMAC DRBG Certificate Generation	Crypto Officer - AES-GCM Key: E - Access

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
			or set CA certificate		Certificate Verification Entropy Source	Token: R,W,Z - ECDSA Public Key: G,R - ECDSA Public Key Certificate: W - CA Certificate: W - DRBG V: W,E - DRBG Key: W,E - ECDSA Private Key: G - ECDSA Self-signed Certificate: G,W,Z - Entropy Input: E
Firmware Upload	Upload device firmware that may contain a new build server public key	Function returns without error	Request to upload and install new firmware or get install process	Response containing upload or install process status	TLS Payload Encryption TLS KTS Factory Pre-load	Crypto Officer - AES-GCM Key: E - Access Token: R,W,Z - Build Server Public Key: W,E
Module Management	Configuration of the module	Function returns without error	Request to get or set module parameters	Response containing parameters or status of the set action	TLS Payload Encryption	Crypto Officer - AES-GCM Key: E - Access Token: R,W,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
On-demand Integrity Test	Perform integrity self-test	ALM LED blinks, function returns without error	Request to run integrity self-test	ALM LED blinks and Response containing integrity test status (test is running, test passed, or test failed)	TLS Payload Encryption	Crypto Officer - AES-GCM Key: E - Access Token: R,W,Z
On-demand Self-test	Perform self-test	ALM LED blinks, function returns without error	Request to run self-test besides integrity	ALM LED blinks and Response containing self-test status (test is running, test passed, or test failed)	TLS Payload Encryption	Crypto Officer - AES-GCM Key: E - Access Token: R,W,Z
Reset	Reset the device to factory default	SEC LED blinks, function returns without error	Request to reset or tamper switch triggered	SEC LED blinks (begin boot sequence) and Device reset to factory default	TLS Payload Encryption Module Reset	Crypto Officer - AES-GCM Key: E - Access Token: R,W,Z
Show Status	Return status of the module	Function returns without error	Request for the status of the module	SEC LED on Response containing module status and peripheral hardware status	TLS Payload Encryption	Crypto Officer - AES-GCM Key: E - Access Token: R,W,Z
Show Version	Return version and name of the module	Function returns without error	Request for the module version	Response containing the module version and name	TLS Payload Encryption	Crypto Officer - AES-GCM Key: E - Access

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Token: R,W,Z
Zeroisation	Zeroize all SSPs	SEC LED blinks, function returns without error	Request for zeroization or tamper switch triggered	SEC LED blinks and device set to factory default	TLS Payload Encryption	Crypto Officer - AES-GCM Key: E,Z - ECDSA Private Key: Z - ECDSA Public Key: Z - ECDSA Public Key Certificate: Z - ECDSA Self-signed Certificate: Z - CA Certificate: Z - Operator Certificate: Z - Hashed Password: Z - Access Token: Z - DRBG Key: Z - DRBG V: Z
SNMPv3	Transmit network polling metrics data via non-approved SNMPv3 protocol	Response with network metrics	Request for network metrics	Response with network metrics	None	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Set Password	Set or update a user password	Function returns without error	Request to set user password	Response containing status of the set action	Password Hash	Crypto Officer - Hashed Password : G

Table 12: Approved Services

The Roles SSP Access column has entries for each SSP accessed by that role using that service with the appropriate access indicators:

- G: The module generates or derives the SSP.
- R: The SSP is read from the module (e.g. the SSP is output).
- W: The SSP is updated, imported, or written to the module.
- E: The module uses the SSP in performing a cryptographic operation.
- Z: The module resets the SSP to zero.

The module provides services to operators who assume one of the roles. Only approved services are offered.

Build Server Public Key is pre-loaded by manufacturer and new firmware may contain a new key for validating the next firmware.

4.4 Non-Approved Services

N/A for this module.

4.5 External Software/Firmware Loaded

There are two main integrity mechanisms: one for updating packages and one runtime. Both mechanisms rely on:

1. The build server having a local only private key, and
2. The build server's public key being embedded into the primary application at compilation time.

The build server builds the primary application then creates a signature file for it. For other files in an update, corresponding signature files are created (which may be combined). These files are then bundled into a single update file that will also be signed by the build server. At this point, the update file is securely transferred to a customer for update.

An operator acting as the Crypto Officer then uses the REST API and an admin token to send the package to the device. The device will first verify the package file has been signed by the trusted build server, else it will not proceed. It will then install the primary application and other files to their desired directories. Finally, it will fail over the new code and trigger a runtime integrity check.

A runtime integrity check will be performed at boot. It will first find the signature file for the primary application and verify its own integrity before proceeding. It will verify the integrity of all files in other signature files. Assuming all the files pass this verification the integrity check passes.

Only firmware validated by the CMVP shall be loaded to maintain module validation. Loading firmware updates that have not been validated means the module is no longer a validated module.

4.6 Bypass Actions and Status

The Port Authority does not support bypass capability.

5 Software/Firmware Security

5.1 Integrity Techniques

The software components of the module are validated by using a Digital Signature (ECDSA P-256) approved technique. A runtime integrity check will be performed at boot automatically and can be run on demand. It will first find the signature file for the primary application and verify its own integrity before proceeding. It will verify the integrity of all files in other signature files. If all the files pass this verification the integrity check passes.

5.2 Initiate on Demand

The module provides on-demand integrity test. The integrity test is performed by the On-demand Integrity test service, which is called on request and verifying the signature as explained in the Integrity Techniques section.

6 Operational Environment

6.1 Operational Environment Type and Requirements

The Port Authority uses a limited operational environment. The code is stored in a FLASH chip in binary executable format. A Crypto Officer can only modify the existing code in the Port Authority by issuing an authenticated update command with a signed firmware package.

Type of Operational Environment: Limited

6.2 Configuration Settings and Restrictions

The module should be installed as stated in section 11.

7 Physical Security

7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
Tamper Seal	12 months	A pristine tamper evident seal appears smooth and uniform, firmly adhering to the surface of the device. By closely examining the seal, one can determine whether any tampering has occurred. Attempted removal of the seal may exhibit one or more of the following signs: 1) The silver adhesive layer displays separation or irregularities, forming a noticeable pattern. The printed text may become separated or misaligned from the silver adhesive layer. 2) Blistering, bubbling, or the presence of bumps on the seal's surface, causing it to lose its smooth and flat appearance. These surface irregularities may become apparent when tilting the seal in the light. 3) The edges of the seal show signs of lifting or failing to stay adhered. It can be easily lifted by gently sliding a pick or fingernail under its edge. 4) Residue of adhesive is detectable around the edges of the seal, indicating it has been removed and replaced.
Tamper Switch	N/A	The tamper switch will trip if an attempt is made to remove the top cover. The top cover for all units 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, keys and operator information will be zeroed. The zeroization circuit will activate regardless of if the SRAM is powered by the battery backup or powered by AC.

Table 13: Mechanisms and Actions Required

The Port Authority series module is a multi-chip standalone cryptographic module, consisting of a number of IC chips mounted on a printed circuit board contained within a protected enclosure. The enclosure contains tamper seals that will be destroyed if an attempted is made to remove them.

Each cryptographic module has a number of tamper evident seals applied as shown in the following section.

7.2 User Placed Tamper Seals

Number:

- PA111-SA: 2 tamper seals
- PA111-RM, PA121-RM, PA155-RM, PA199-RM: 4 tamper seals

Placement:

- middle of left side and right side (all models)
- middle of front seam (PA111-RM, PA121-RM, PA155-RM, and PA199-RM)
- middle of back seam (PA111-RM, PA121-RM, PA155-RM, and PA199-RM)

Surface Preparation: cleaned with alcohol before placement

Operator Responsible for Securing Unused Seals: Crypto Officer

Part Numbers: NOVA Vision XUG6-K222-60S

PA111-SA

Figure 11: PA111-SA Tamper Seal at Side/Bottom

Figure 12: PA111-SA Tamper Seal at Side/Bottom

PA121-RM

Figure 13: PA121-RM Tamper Seals at Side/Bottom and Front/Bottom

Figure 14: PA121-RM Tamper Seals at Side/Bottom and Rear/Top

PA111-RM, PA155-RM, and PA199-RM

Figure 15: PA111-RM, PA155-RM, PA199-RM Tamper Seals at front/Top and Side/Bottom

Figure 16: PA111-RM, PA155-RM, PA199-RM Tamper Seals at Rear/Bottom

8 Non-Invasive Security

The module does not implement any non-invasive mitigation techniques.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
Flash	Port Authority non-volatile memory	Static
RAM	Port Authority working memory	Dynamic
SRAM	Port Authority backup memory	Dynamic

Table 14: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Factory Pre-load	Manufacturer	Flash	Plaintext	N/A	N/A	Factory Pre-load
Load Cert	Outside the crypto boundary	SRAM	Plaintext	Manual	Electronic	TLS KTS
Operator Password Entry	Outside the crypto boundary	RAM	Encrypted	Manual	Electronic	TLS Payload Encryption
Operator Set Password Entry	Outside the crypto boundary	SRAM	Encrypted	Manual	Electronic	TLS Payload Encryption
Token-In	Outside the crypto boundary	RAM	Encrypted	Automated	Electronic	TLS Payload Encryption
Token-Out	RAM	Outside the crypto boundary	Encrypted	Automated	Electronic	TLS Payload Encryption

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
TLS Handshake-In	Outside the crypto boundary	RAM	Plaintext	Automated	Electronic	
TLS Handshake-Out	RAM	Outside the crypto boundary	Plaintext	Automated	Electronic	
TLS Payload-In	Outside the crypto boundary	RAM	Encrypted	Automated	Electronic	TLS Payload Encryption
TLS Payload-Out	RAM	Outside the crypto boundary	Encrypted	Automated	Electronic	TLS Payload Encryption

Table 15: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Reset	Reset to factory default	SSPs are zeroed when the operator invokes the service	Operator may use module control input to reset the module to factory state
Zeroization	Zeroization of persistent SSPs	SSPs are zeroed when the operator invokes the service	Operator may use module control input to reset the module
Tamper Response	Zeroization of all SSPs	All SSPs are zeroed when tamper switch is tripped	Operator may open the enclosure that causes the module to zeroize all SSPs and reset to factory state
Power Cycle	Power cycle the module	All ephemeral SSPs in RAM will be destroyed	Operator may use control input to restart the module
Session Termination	Zeroization of ephemeral SSPs	Ephemeral SSPs related to TLS protocol are zeroed when connection closed	Operator may perform actions that cause a TLS session to terminate
Function Exit	Zeroization of ephemeral SSPs	Ephemeral SSPs generated within a function are zeroed when the function returns	No operator initiation

Table 16: SSP Zeroization Methods

Notes:

1. Server public key outputs as certificate signing request.
2. Only Crypto Officer can create new operator (Crypto Officer or User) and set the password for the operator. The module does not allow User to change password; only Crypto Office can change password on behalf of User.

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
AES-GCM Key	Session key for TLS connection	128, 256 - 128-256	Symmetric Key - CSP		TLS Key Agreement	TLS Payload Encryption TLS KTS
TLS Premaster Secret	Premaster secret for TLS connections	384 - 128-256	Shared Secret - CSP		TLS Key Agreement	TLS Key Agreement
TLS Master Secret	Master secret for TLS connections	384 - 128-256	Shared Secret - CSP		TLS Key Agreement	TLS Key Agreement
EC Diffie-Hellman Private Key	Private key for KAS-ECC for TLS	P-256 - 128	Private - CSP	TLS Key Agreement		TLS Key Agreement
EC Diffie-Hellman Public Key	Public key for KAS-ECC for TLS	P-256 - 128	Public - PSP	TLS Key Agreement		
Peer EC Diffie-Hellman Public Key	Public key for KAS-ECC for TLS	P-256 - 128	Public - PSP			TLS Key Agreement
ECDSA Private Key	Server private key used to sign parts of the TLS handshake messages and access token	P-256 - 128	Private - CSP	Certificate Generation		TLS Server Authentication SigGen
ECDSA Public Key	Server public key generated within the module as part of certificate generation and used to	P-256 - 128	Public - PSP	Certificate Generation		SigVer

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	verify access token					
ECDSA Public Key Certificate	CA signed certificate containing the server public key, hostname, and other identifying information	P-256 - 128	Public - PSP			TLS Server Authentication
ECDSA Self-signed Certificate	Self-signed certificate containing the server public key, hostname, and other identifying information	P-256 - 128	Public - PSP	Module Reset		TLS Server Authentication
CA Certificate	CA public key certificate used to verify the trusted chain of certificate	P-256 - 128	Public - PSP			TLS Server Authentication Certificate Verification Certificate Authentication
Build Server Public Key	ECDSA public key used to verify firmware integrity and update package that may contain a new build server public key	P-256 - 128	Public - PSP			Factory Pre-load
DRBG V	SP 800-90A HMAC_DRBG V	256 - 128	DRBG internal state - CSP	HMAC DRBG		HMAC DRBG
DRBG Key	SP 800-90A HMAC_DRBG Key	256 - 128	DRBG internal state - CSP	HMAC DRBG		HMAC DRBG

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Entropy Input	Input from the SP 800-90B entropy source	440 - 128	Entropy - CSP	Entropy Source		HMAC DRBG
Password	Credential for operator authentication	Minimum of 8 characters - N/A	Password - CSP			Password Authentication
Hashed Password	Password hash	256 - N/A	Password - CSP			Password Authentication
Operator Certificate	Public key certificate for operator authentication	P-256 - 128	Public - PSP			Certificate Authentication
Access Token	Time-limited access token signed by the module's ECDSA Private Key	P-256 - 128	Signature - CSP	Certificate Authentication Password Authentication		

Table 17: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
AES-GCM Key		RAM:Plaintext	Session lifetime	Reset Zeroization Tamper Response Power Cycle Session Termination	TLS Master Secret :Derived From
TLS Premaster Secret		RAM:Plaintext	Session lifetime	Reset Zeroization Tamper Response Power Cycle Session Termination	EC Diffie-Hellman Private Key:Used With Peer EC Diffie-Hellman Public Key:Used With TLS Master Secret :Used to Derive
TLS Master Secret		RAM:Plaintext	Session lifetime	Reset Zeroization Tamper Response Power Cycle	TLS Premaster Secret :Derived From AES-GCM Key:Derives

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				Session Termination	
EC Diffie-Hellman Private Key		RAM:Plaintext	Session lifetime	Reset Zeroization Tamper Response Power Cycle Session Termination	EC Diffie-Hellman Public Key :Paired With Peer EC Diffie-Hellman Public Key:Used With TLS Premaster Secret :Agrees Upon DRBG Key:Used With DRBG V:Used With
EC Diffie-Hellman Public Key	TLS Handshake-Out	RAM:Plaintext	Session lifetime	Reset Zeroization Tamper Response Power Cycle Session Termination	EC Diffie-Hellman Private Key:Paired With DRBG Key:Used With DRBG V:Used With
Peer EC Diffie-Hellman Public Key	TLS Handshake-In	RAM:Plaintext	Session lifetime	Reset Zeroization Tamper Response Power Cycle Session Termination	EC Diffie-Hellman Private Key:Used With TLS Premaster Secret :Agreed Upon
ECDSA Private Key		SRAM:Plaintext		Reset Zeroization Tamper Response	ECDSA Public Key Certificate:Paired With ECDSA Public Key:Paired With ECDSA Self-signed Certificate:Paired With
ECDSA Public Key	TLS Handshake-Out TLS Payload-Out	SRAM:Plaintext		Reset Zeroization Tamper Response	ECDSA Private Key:Paired With
ECDSA Public Key Certificate	Load Cert TLS	SRAM:Plaintext		Reset Zeroization	ECDSA Private Key:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	Handshake-Out			Tamper Response	
ECDSA Self-signed Certificate	TLS Handshake-Out	SRAM:Plaintext		Reset Zeroization Tamper Response	ECDSA Private Key:Paired With
CA Certificate	Load Cert TLS Handshake-Out	SRAM:Plaintext		Reset Zeroization Tamper Response	Operator Certificate:Used With
Build Server Public Key	Factory Pre-load TLS Payload-In	Flash:Plaintext		N/A	
DRBG V		RAM:Plaintext	Module powered up	Reset Zeroization Tamper Response Power Cycle Function Exit	Entropy Input:Derived From
DRBG Key		RAM:Plaintext	Module powered up	Reset Zeroization Tamper Response Power Cycle Function Exit	Entropy Input:Derived From
Entropy Input		RAM:Plaintext	Module powered up	Reset Zeroization Tamper Response Power Cycle Function Exit	DRBG Key:Input To Seed DRBG V:Input To Seed
Password	Operator Password Entry Operator Set Password Entry	RAM:Plaintext	Session lifetime	Reset Zeroization Tamper Response Power Cycle Function Exit	
Hashed Password		RAM:Plaintext	Session lifetime	Reset Zeroization	Password :Hash Of

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				Tamper Response Power Cycle Function Exit	
Operator Certificate	TLS Handshake-In	RAM:Plaintext	Session lifetime	Reset Zeroization Tamper Response Power Cycle Session Termination	CA Certificate:Used With
Access Token	Token-In Token-Out	RAM:Plaintext	Token lifetime	Reset Zeroization Tamper Response Power Cycle Session Termination	ECDSA Private Key:Signed By ECDSA Public Key:Used With

Table 18: SSP Table 2

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
Firmware Integrity Test	ECDSA signature verification	Signature Verification	SW/FW Integrity	SEC LED blinking and "passed test: SelfIntegrityTest" in log file	Firmware integrity

Table 19: Pre-Operational Self-Tests

The module performs pre-operational self-test automatically when the module powers on. The ECDSA SigVer and SHA2-256 conditional known answer tests are performed before performing the pre-operational module integrity test. The integrity of the software component is then verified according to section 5, using a digital signature. If the known answer test or integrity test fails, the module transits to the Error state.

The module also performs the cryptographic algorithms self-tests and critical function test defined in section 10.2.

In addition, the CDI CPU Time Jitter entropy source performs start-up health testing as part of the Critical Function Tests.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB (A4440)	128, 256	KAT	CAST	"passed test: SelfTestECB" in log file	Encrypt & Decrypt	Power-up
AES-GCM (A4440)	128, 256	KAT	CAST	"passed test: SelfTestGCM" in log file	Encrypt & Decrypt	Power-up
ECDSA KeyGen (FIPS186-4) (A4440)	P-256	PCT	PCT	N/A	Sign & Verify	Keypair generation
ECDSA SigGen (FIPS186-4) (A4440)	P-256	KAT	CAST	"passed test: SelfTestECDSA" in log file	Sign	Power-up
ECDSA SigVer (FIPS186-4) (A4440)	P-256	KAT	CAST	"passed test: SelfTestECDSA" in log file	Verify	Power-up
HMAC DRBG (A4440)	HMAC-SHA2-256	KAT	CAST	"passed test: SelfTestDRBG" in log file	SP 800-90Ar1 11.3 Instantiate, Reseed, Generate chained test	Power-up
HMAC-SHA-1 (A4440)	N/A	KAT	CAST	"passed test: SelfTestHMACSHA1" in log file	HMAC	Power-up
HMAC-SHA2-256 (A4440)	N/A	KAT	CAST	"passed test: SelfTestHMAC" in log file	HMAC	Power-up
HMAC-SHA2-384 (A4440)	N/A	KAT	CAST	"passed test: SelfTestHMAC" in log file	HMAC	Power-up
KAS-ECC-SSC Sp800-56Ar3 (A4440)	P-256	KAT	CAST	"passed test: SelfTestECCSSC" in log file	Shared Secret Computation	Power-up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA-1 (A4440)	SHA-1	KAT	CAST	"passed test: SelfTestSHA1" in log file	Hash	Power-up
SHA2-256 (A4440)	SHA2-256	KAT	CAST	"passed test: SelfTestSHA" in log file	Hash	Power-up
SHA2-384 (A4440)	SHA2-384	KAT	CAST	"passed test: SelfTestSHA" in log file	Hash	Power-up
TLS v1.3 KDF (A4440)	SHA2-256, SHA2-384	KAT	CAST	"passed test: SelfTestKDF-TLS" in log file	KDF	Power-up
SHA3-256 (A3214)	SHA3-256	KAT	CAST	"passed test: SelfTestSHA3" in log file	Hash	Power-up

Table 20: Conditional Self-Tests

Cryptographic Algorithm Self-Tests
The module performs self-tests on approved cryptographic algorithms supported in the approved mode of operation. Data output is inhibited during the self-tests. The cryptographic algorithm self-tests are performed in the form of Known Answer Tests (KATs), in which the calculated output is compared with the expected known answer.

The module performs testing on the continuous outputs of the entropy source. The CDI CPU Time Jitter entropy source executes the APT, RCT and Lag tests as approved health testing. If any of these self-tests fails, the module transitions to the Error state.

Conditional Pairwise Consistency Tests
The module implements the ECDSA algorithm and key generation and performs the pairwise consistency test using sign and verify functions when the keys are generated.
In addition, the assurance for the KAS-ECC-SSC (per section 5.6.2 of SP 800-56Arev3, required by [IG] D.F) is verified by running conditional testing on the ephemeral key pairs created during the key agreement.

Conditional Software/Firmware Load Test
When the module receives an update as a result of the execution of the Firmware Upload service, the conditional software load test is executed and the module applies a digital signature integrity technique to verify the validity of the firmware.

Conditional Manual Entry Test
When setting or changing a password, the module uses duplicate entries to prevent error on the part of the human operator could result in the incorrect entry of the intended value.

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Firmware Integrity Test	Signature Verification	SW/FW Integrity	Module operational	Module restart, On-demand Integrity Test or Self, or On-demand Self-test

Table 21: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-ECB (A4440)	KAT	CAST	Module operational	Power-up and On-demand
AES-GCM (A4440)	KAT	CAST	Module operational	Power-up and On-demand
ECDSA KeyGen (FIPS186-4) (A4440)	PCT	PCT	N/A	N/A
ECDSA SigGen (FIPS186-4) (A4440)	KAT	CAST	Module operational	Power-up and On-demand
ECDSA SigVer (FIPS186-4) (A4440)	KAT	CAST	Module operational	Power-up and On-demand
HMAC DRBG (A4440)	KAT	CAST	Module operational	Power-up and On-demand
HMAC-SHA-1 (A4440)	KAT	CAST	Module operational	Power-up and On-demand
HMAC-SHA2-256 (A4440)	KAT	CAST	Module operational	Power-up and On-demand
HMAC-SHA2-384 (A4440)	KAT	CAST	Module operational	Power-up and On-demand
KAS-ECC-SSC Sp800-56Ar3 (A4440)	KAT	CAST	Module operational	Power-up and On-demand
SHA-1 (A4440)	KAT	CAST	Module operational	Power-up and On-demand
SHA2-256 (A4440)	KAT	CAST	Module operational	Power-up and On-demand
SHA2-384 (A4440)	KAT	CAST	Module operational	Power-up and On-demand
TLS v1.3 KDF (A4440)	KAT	CAST	Module operational	Power-up and On-demand
SHA3-256 (A3214)	KAT	CAST	Module operational	Power-up and On-demand

Table 22: Conditional Periodic Information

On demand self-tests can be invoked by executing the services On-demand Self-tests and On-demand Integrity test. The services request the self-test after the boot initialization sequence.

During the execution of the on-demand self-tests, cryptographic services are not available, and no data output or input is possible.

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Error	Any pre-operational self-test, cryptographic algorithms self-tests, or critical function test failure	Initialization error, self-test error or general error from any state lead to the Error state	Reboot or hard reset	ALM LED on

Table 23: Error States

If the module fails any of the self-tests or receives an error from the system initialization or any other operational state, the module outputs an error and stops functioning, and the output interface is inhibited as well. To recover from the Error state, the operator must perform a reboot or hard reset, and the module will execute all the pre-operational self-tests again.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The base image and the primary applications are installed at factory and no other startup steps are needed.

11.2 Administrator Guidance

CDI will send a serial number list electronically and securely to the customer. When the module is delivered the Crypto Officer can compare the serial number of the module against the list CDI provided and check against tampering following the Inspection/Test Guidance in Section 7.1. If any tamper evident seal is damaged, the Crypto Officer shall contact manufacturer to replace the module.

The module requires the Crypto Officer to reset the default the CO password upon accessing the module for the first time or after a hard reset. The Crypto Officer should choose a password of minimum length of 8 characters with sufficient complexity and secrecy.

The Crypto Officer should check the name and version information matches the following by a request to “/v1/fips/versions”:

{"Hardware":"PA111","FirmVer":"1.0.0","BldVer":"F13-1","RepoVer":"
c406cc110c5c8422440c8a6ca79838238ae8f5ea "},
{"Hardware":"PA121","FirmVer":"1.0.0","BldVer":"F13-1","RepoVer":"
c406cc110c5c8422440c8a6ca79838238ae8f5ea "},
{"Hardware":"PA155","FirmVer":"1.0.0","BldVer":"F13-1","RepoVer":"

c406cc110c5c8422440c8a6ca79838238ae8f5ea "}, or
{"Hardware":"PA199","FirmVer":"1.0.0","BldVer":"F13-1","RepoVer":"
c406cc110c5c8422440c8a6ca79838238ae8f5ea "}

The Crypto Officer is in charge of executing the Firmware Upload service when an update is released. The CO shall only upload firmware validated by the CMVP.

If a tamper evident seal is damaged by accident, the CO shall replace the damaged seal following the instructions illustrated in Section 7.

11.3 Non-Administrator Guidance

There is no specific procedures for non-administrator operators.

11.4 End of Life

To decommission the module, the CO shall execute the Reset/Zeroization service. This process will erase all SSPs contained within the cryptographic module. After that, the module shall be disposed of or distributed to other operators.

12 Mitigation of Other Attacks

The module does not mitigate other attacks outside the scope of FIPS 140-3.