Communication Devices, Inc.

Port Authority Series

Hardware Version:
PA111-SA CDI 01-03-0912I
PA111-RM CDI 01-03-0912I
PA121-RM CDI 01-03-0912I
PA155-RM CDI 01-03-0912I
PA199-RM CDI 01-03-0912I

Firmware Version:
1.0.0

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

Document Version: 1.2

Date: 9/6/2024

Table of Contents

1 General Information

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

ISO/IEC 24759 Section 6	FIPS 140-3 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

Table 1: Security Levels

Overall security level 2.

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: None

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:

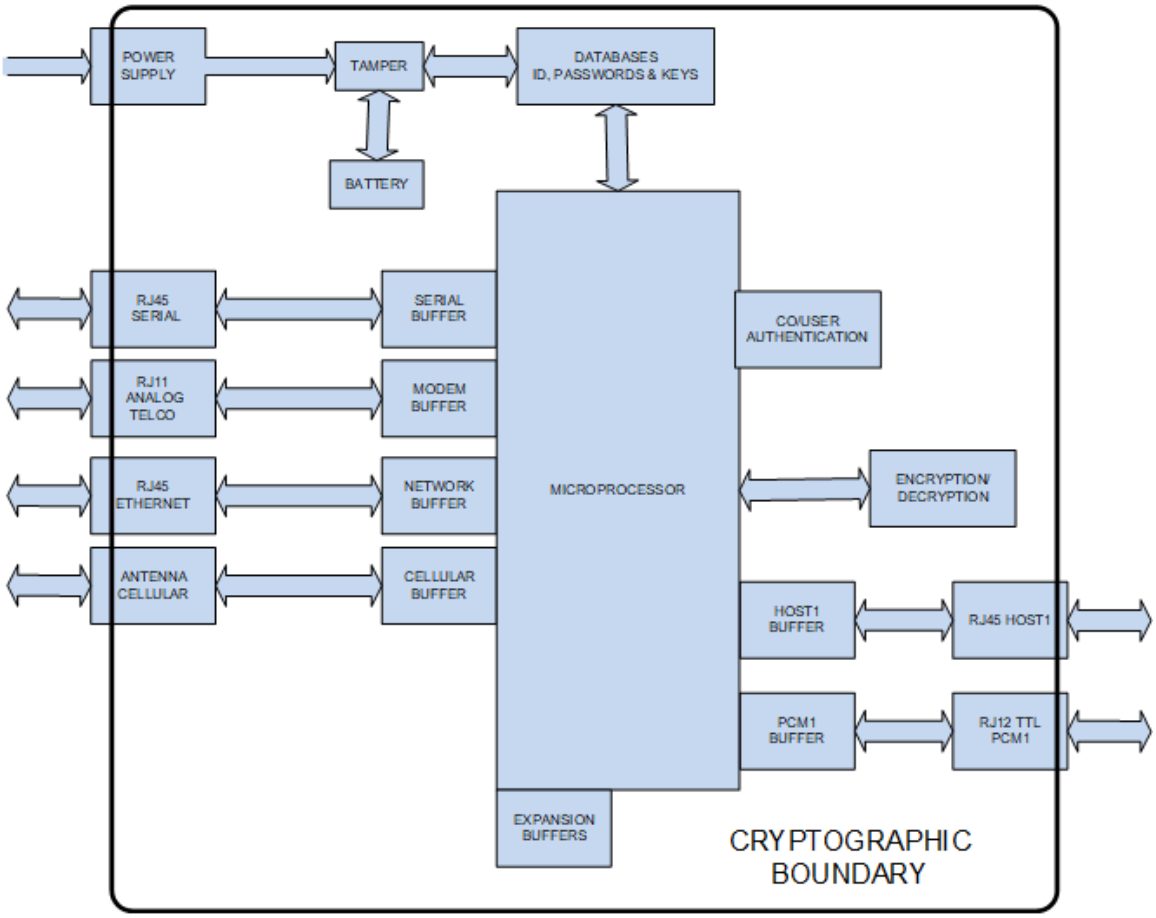

Figure 1: Block Diagram Depicting the Cryptographic Boundary

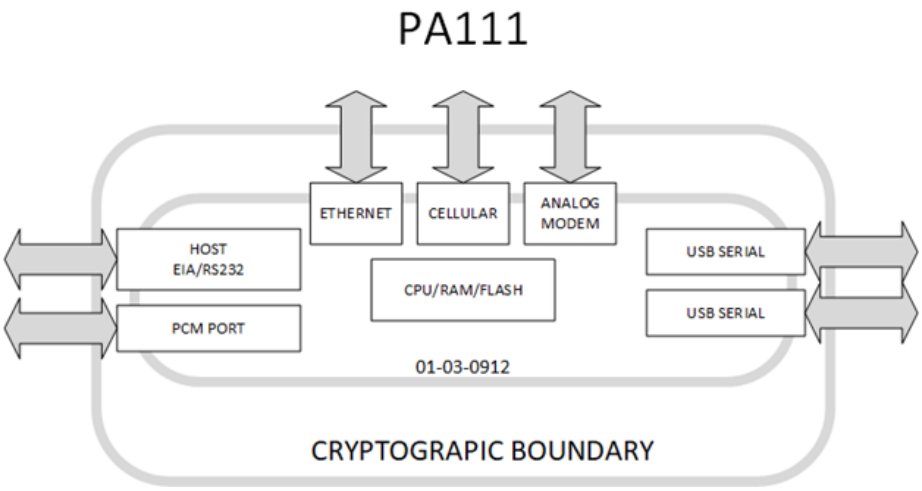

Figure 2: PA111-SA and PA111-RM Hardware Diagram

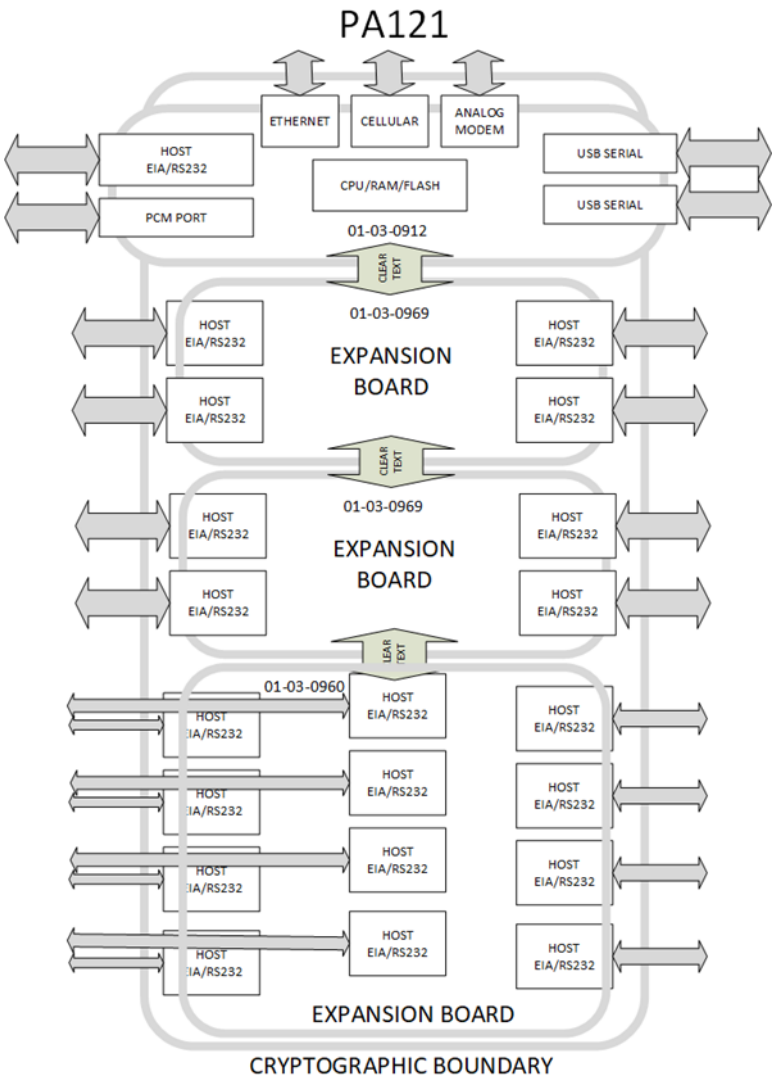

Figure 3: PA121 Hardware Diagram

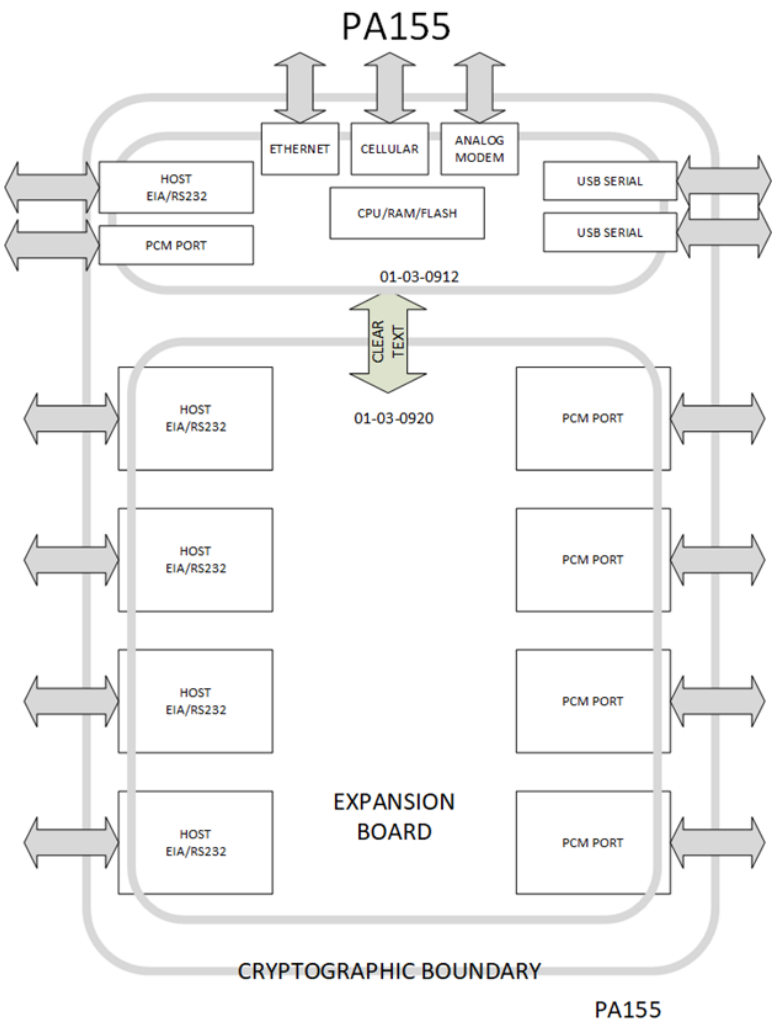

Figure 4: PA155 Hardware Diagram

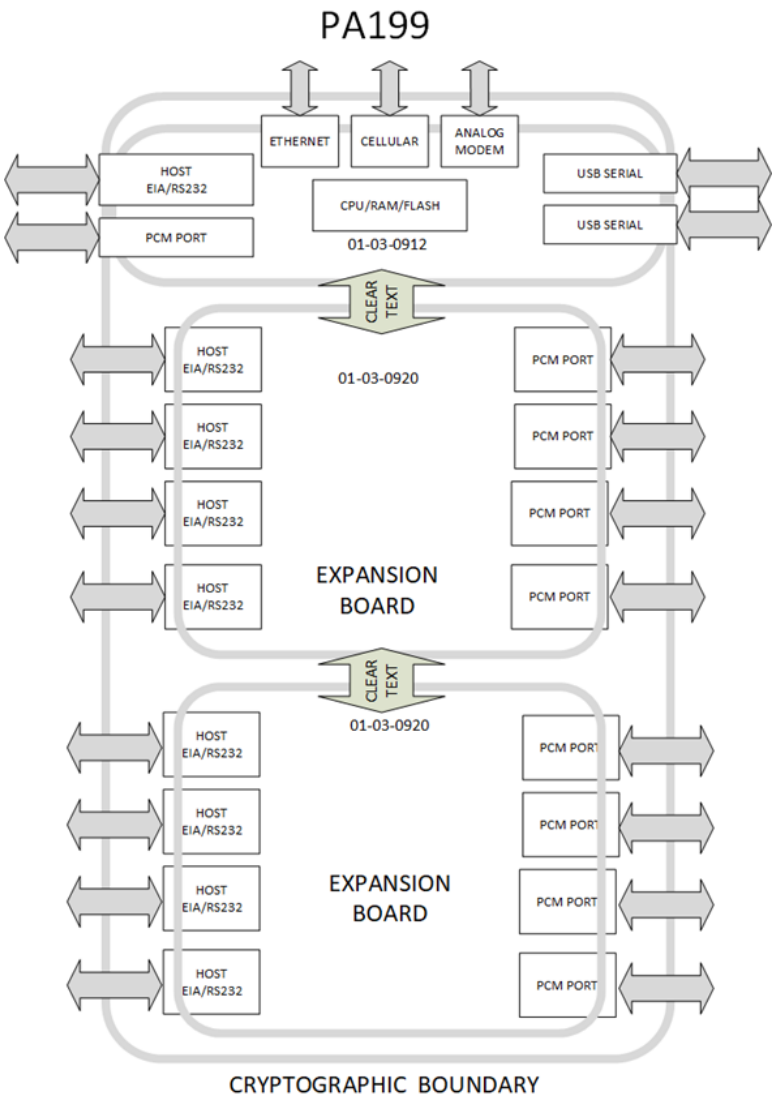

Figure 5: PA199 Hardware Diagram

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

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

Tested Module Identification - Hardware:

Model/Part Number	Hardware Version	Firmware Version	Processor	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

2.3 Excluded Components

There are no excluded components for this cryptographic module.

2.4 Modes of Operation

Modes List and Description:

Name	Description	Type	Status Indicator
Approved mode	The module only supports the approved mode of operation	Approved	SEC LED on

Table 3: Modes of Operation

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 changes instructions and status indicators

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

Degraded Mode Description

The module does not implement degraded operation.

2.5 Algorithms

The table below 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.

CAVP Cert	Algorithm and Standard	Mode/Method	Description / Key Size(s) / Key Strength(s)	Use / Function
A3214	SHA-3 [FIPS 202]	SHA3-256		Conditioning

CAVP Cert	Algorithm and Standard	Mode/Method	Description / Key Size(s) / Key Strength(s)	Use / Function
				function
A4440	AES [SP 800-38A]	ECB[1]	128 and 256-bit keys with 128 and 256-bit key strengths	Encrypt/Decrypt
A4440	AES [SP 800-38D]	GCM	128 and 256-bit keys with 128 and 256-bit key strengths	Encrypt/Decrypt
A4440	DRBG [SP 800-90A]	HMAC DRBG	SHA2-256 with 128-bit key strength	Deterministic Random Bit Generation
A4440	ECDSA [FIPS 186-4]	KeyGen	P-256 with 128-bit key strength	Asymmetric Key Generation
A4440	ECDSA [FIPS 186-4]	KeyVer	P-256 with 128-bit key strength	Asymmetric Key Verification
A4440	ECDSA [FIPS 186-4]	SigGen	P-256/SHA2-256 with 128-bit key strength	Signature Generation
A4440	ECDSA [FIPS 186-4]	SigVer	P-256/SHA2-256 with 128-bit key strength	Signature Verification
E100	ESV [SP 800-90B]	CPU Jitter Source	CDI CPU Time Jitter, 8-bit samples	Non-Deterministic Random Bit Generation
A4440	HMAC [FIPS 198-1]	HMAC[2]	SHA-1 / 128 – 1024-bit keys with 112-bit key strength, SHA2-256 / 256 – 512-bit keys with 128-bit key strength, SHA2-384 / 256 – 512-bit keys with 192-bit key strength	Message Authentication
A4440	KAS [SP 800-56Arev3]	KAS-ECC-SSC [SP 800-56Arev3]/A4440 TLS 1.3 KDF/A4440	P-256 with 128-bit key strength	TLS key agreement
A4440	KAS-ECC-SSC [SP 800-56Arev3]	Ephemeral Unified	P-256 with 128-bit key strength	Shared Secret Computation for Key Agreement
A4440	SHS [FIPS 180-4]	SHA-1[3], SHA2-256, SHA2-384		Message Digest
A4440	TLS 1.3 KDF [RFC 8446] CVL	HMAC-SHA2-256, HMAC-SHA2-384		Key Derivation Function No parts of these

[1] AES-ECB is CAVP tested but not used by the module. This algorithm can only be executed when running a self-test

[2] HMAC-SHA-1 is CAVP tested but not used by the module.

[3] SHA-1 is CAVP tested but not used by the module.

CAVP Cert	Algorithm and Standard	Mode/Method	Description / Key Size(s) / Key Strength(s)	Use / Function
				protocols, other than the approved cryptographic algorithms and the KDFs, have been tested by the CAVP and CMVP.

Table 4: Approved 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.

Vendor-Affirmed Algorithms

The table below lists the vendor affirmed algorithms that are allowed in the approved mode of operation.

Name	Properties	Implementation	Reference
CKG		Cryptographic key generation per SP 800-133rev2 and IG D.I - Generation of asymmetric keys for signature generation per [133] section 5.1. - Generation of asymmetric keys for key establishment per [133] section 5.2. - Symmetric key derivation for industry standard protocols from a key agreement shared secret per [133] section 6.2.1.	IG.D.H

Table 5: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms

The module does not implement any non-approved security functions that are allowed in approved services.

Non-Approved, Allowed with No Security Claimed

The module implements the SNMPv3 protocol which is 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 transmits over the SNMP protocol only contains network metrics data that is non-sensitive and is considered plaintext.

Name	Caveat	Use and Function
AES-CFB8	Network metrics output over SNMPv3 protocol is obfuscated and considered plaintext	SNMPv3 privacy protocol
SNMP KDF	Key localization function uses a SHA2-256 hash function not	SNMPv3 key derivation

	the SHA-1 specified in SP 800-135r1	

Table 6: Non-Approved Allowed in the Approved Mode of Operation with No Security Claimed

Non-Approved, Not Allowed Algorithms

The module does not implement any non-approved security functions that are not allowed in approved services.

2.6 Security Function Implementation

Name	Type	Description	Properties	Algorithms
KAS-ECC	KAS	Uses the KAS-ECC-SSC shared secret computation which is then fed into the module's TLS 1.3 KDF to derive keys for the TLS 1.3 protocol	IG D.F scenario 2, path (2), no key confirmation, key derivation per IG 2.4.B, resolution (7). P-256 curve providing 128 bits of encryption strength	KAS-ECC-SSC SP 800-56Ar3/A4440 TLS v1.3 KDF/A4440
TLS-KTS	KTS	PSP transmitted as TLS payload	SP 800-38D and SP 800-38F. KTS (key wrapping and unwrapping), per IG D.G., providing 128 bits of encryption strength	AES-GCM/A4440

Table 7: Security Function Implementation (SFI)

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}.

In the event the module's power is lost and restored, the module will establish a new key for use with the AES-GCM encryption/decryption.

2.8 RNG and Entropy

Name	Type	Operating Environment	Sample Size	Entropy per Sample	Conditioning Component
CDI CPU Time Jitter	Non-Physical	Linux 4.14, i.MX6 Ultralite (NXP, IMX6, ARM32)	8 bits	1	SHA3-256 (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 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 with 128 bits of encryption strength. 440 bits of entropy input is used to seed the DRBG.

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[4].

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[5] 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_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256			
	ECDH	ECDSA	AES-GCM	SHS
	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384			
	ECDH	ECDSA	AES-GCM	SHS

Table 9: Security Relevant Protocols

2.12 Design and Rules

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.

2.13 Initialization

No guidance for initialization is declared.

[4] This SNMP KDF is a non-approved algorithm used by the module as a non-security function with no security claimed.

[5] 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.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface	Data that passes over the port/interface
LEDs	• Status Output	Device Status
Network	• Control Input • Control Output* • Status Output	CO traffic
	• Data Input • Data Output	User traffic
Cellular Antennas	• Control Input • Control Output* • Status Output	CO traffic
	• Data Input • Data Output	User traffic
Telco	• Control Input • Control Output* • Status Output	CO traffic
	• Data Input • Data Output	User traffic
Host(s)	• Data Input	User traffic from managed device
	• Data Output	User traffic to managed device
PCM(s)	• Control Output	User traffic to Power Control Module
Console	• Control Input • Status Output	CO traffic
Reset Switch	• Control Input	Hardware reset signal
Power(s)	• Power	VAC and VDC
USBs	• Data Input	User traffic from managed device
	• Data Output	User traffic to managed device

Table 10: 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 Trusted Channel Specification

The module does not implement any trusted channels.

3.3 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

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 ($400/95^8$).

Name	Description	Mechanism	Strength of Each Attempt	Strength per Minute
Certificate	X509v3 for CO and User roles	Signature Verification	2^{128}	$8.8x10^{-17}$
Credential	ID and Password for CO and User roles over analog	Identity-based authentication	95^8	$4.5x10^{-15}$

Credential	ID and Password for CO and User roles over cellular	Identity-based authentication	95[8]	$6.0x10^{-14}$

Table 11: Authentication Methods

4.2 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:

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Identity	CO	Credential, Certificate
User	Identity	User	Credential, Certificate

Table 12: 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

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 and listed below:

Name	Description	Indicator	Inputs	Outputs	Security Function Implementation	Roles	Roles SSP Access
Login	Operator login	Function returns without error	Login request, Password, Operator Certificate	Login failure, login success and access token generated	AES ECDSA SigVer KAS-ECC SHA2-256 TLS KDF	CO User	Access Token: E, R Password: E, Z Operator Certificate: E, Z CA Certificate: E AES-GCM Key: G, E TLS Pre-master Secret: G, E TLS Master Secret: G, E EC Diffie-Hellman Public Key: G, E, R EC Diffie-Hellman Private Key: G, E ECDSA Public Key: G, E, R

Name	Description	Indicator	Inputs	Outputs	Security Function Implementation	Roles	Roles SSP Access
							ECDSA Private Key: G, E
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		CO User	Password: Z AES-GCM Key: E
Audit Log	Download event from the device	Function returns without error	Request for module logs	Response containing module logs		CO	AES-GCM Key: E
Certificate Management	Downloading CSR and uploading certificates and CA certificates	Function returns without error	Request to get a device's CSR, set devices's certificate, or set CA certificate	Response containing a CSR or the status of the set action	HMAC DRBG ECDSA KeyGen ECDSA KeyVer ECDSA SigGen ECDSA SigVer	CO	Certificate: W, Z AES-GCM Key: E
Firmware Upload	Uploading device firmware to be installed	Function returns without error	Request to upload and install new firmware or get install process	Response containing upload or install process status	ECDSA SigVer	CO	AES-GCM Key: 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		CO	Password: W, Z AES-GCM Key: E
On-demand Integrity Test	Perform integrity self-test	ALM LED blinks, function returns without error	Request to run integrity self-test	ALM LED blinks Response containing integrity test status (test is running, test passed, or test	ECDSA SigVer	CO	AES-GCM Key: E

Name	Description	Indicator	Inputs	Outputs	Security Function Implementation	Roles	Roles SSP Access
				failed)			
On-demand Self-test	Perform self-test	ALM LED blinks, function returns without error	Request to run self-test besides integrity	ALM LED blinks Response containing self-test status (test is running, test passed, or test failed)		CO	AES-GCM Key: E
Reset	Reset the device to factory default	SEC LED blinks, function returns without error	Request to reset	SEC LED blinks (begin boot sequence) Device reset to factory default		CO	All SSPs: 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		CO	AES-GCM Key: E
Show Version	Return version and name of the module	Function returns without error	Request for the module version	Response containing the module version		CO	AES-GCM Key: E
Zeroisation	Zeroize all SSPs	SEC LED blinks, function returns without error	Request for zeroization or tamper switch triggered	SEC LED blinks Device set to factory default		CO	All SSPs: Z

Table 13: Approved Services

4.4 Non-Approved Services

The cryptographic module supports the following non-approved services.

Name	Description	Security Functions	Role
Network Metrics	Transmit network polling metrics data via non-approved SNMPv3 protocol		Crypto Officer

Table 14: Non-Approved Services

4.5 External Software/Firmware Loaded

There are two main integrity mechanisms: one for updating packages and one runtime. Both of these 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.

4.7 Cryptographic Output Actions and Status

No output of CSPs are declared for this cryptographic module.

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

The module works in a limited operational environment.

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

Physical security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details

Physical security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
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		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 15: 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 Factory Placed Tamper Seals

The Crypto Officer may replace damaged tamper seals. The Crypto Officer must ensure the module surface is clean and dry before applying the 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

Below are the pictures illustrating the placement of the tamper seals on the modules:

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

Name	Description	Persistence Type
SRAM	Port Authority backup memory	Volatile
Flash	Port Authority non-volatile memory	Non-volatile
RAM	Port Authority working memory	Volatile

Table 16: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
TLS Payload-Out[6]	RAM	Outside the crypto boundary	Encrypted	Manual	Electronic	TLS-KTS
Factory Pre-load[7]	Manufacturer	Flash	Plaintext	N/A	N/A	N/A
KAS-In	Outside the crypto boundary	RAM	Plaintext	Automated	Electronic	KAS-SSC
KAS-Out	RAM	Outside the crypto boundary	Plaintext	Automated	Electronic	KAS-SSC
Load Cert	Outside the crypto boundary	SRAM	Encrypted	Manual	Electronic	TLS-KTS
Operator Password Entry	Outside the crypto boundary	RAM	Encrypted	Manual	Electronic	SHA2-256
Operator Set Password Entry[8]	Outside the crypto boundary	SRAM	Encrypted	Manual	Electronic	SHA2-256
Token-In	Outside the crypto boundary	RAM	Encrypted	Automated	Electronic	ECDSA SigVer
Token-Out	RAM	Outside the crypto boundary	Encrypted	Automated	Electronic	ECDSA SigGen
TLS Handshake-In	Outside the crypto boundary	RAM	Plaintext	Automated	Electronic	N/A
TLS Handshake-Out	RAM	Outside the crypto boundary	Plaintext	Automated	Electronic	N/A
TLS Payload-In	Outside the crypto boundary	RAM	Encrypted	Automated	Electronic	AES

Table 17: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Method	Description	Rationale	Operator Initiation

[6] Server public key outputs as certificate signing request.

[7] Key is pre-loaded by manufacturer and new firmware may contain the key for validating the next firmware.

[8] 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.

			Capability
Reset/Zeroization service	Zeroization of persistent SSPs	SSPs are zeroed when the operator invokes the service	Yes
Tamper response	Zeroization of persistent SSPs	SSPs are zeroed when tamper switch is tripped	N/A
Per connection	Zeroization of ephemeral SSPs	Ephemeral SSPs related to TLS and SNMP protocols are zeroed when connection closed	N/A

Table 18: SSP Zeroization

9.4 SSPs

Name	Description	Size - Strength	Type	Generated By	Established By	Used By
AES-GCM Key / CSP	Session key for TLS connection	128 - 128, 256 - 128	Symmetric key	Derived from TLS Master Secret	TLSv1.3 KDF	TLS
TLS Pre- master Secret / CSP	Pre- master secret for TLS connections	384 – 128	Keying material	N/A	TLS handshake	TLS handshake
TLS Master Secret / CSP	Master secret for TLS connection	384 – 128	Keying material	Internally derived by TLSv3 KDF from TLS Pre-master Secret	N/A	TLS handshake
EC Diffie-Hellman Public Key / PSP	Asymmetric key used during EC Diffie-Hellman	P-256 - 128	Public key	Internal ly generated per SP 800-56Arev3	N/A	KAS-SSC
EC Diffie-Hellman Public Key (operator) / PSP	Asymmetric key used during EC Diffie-Hellman	P-256 – 128	Public key	N/A	N/A	KAS-SSC
EC Diffie-Hellman Private Key / CSP	Asymmetric key used during EC Diffie-Hellman	P-256 – 128	Private key	Internally generated per SP 800-56Arev3	N/A	KAS-SSC
ECDSA Public Key / PSP	Asymmetric key used during TLS authentication	P-256 – 128	Public key	Internally generated per FIPS	N/A	TLS handshake

Name	Description	Size - Strength	Type	Generated By	Established By	Used By
				186-4		
ECDSA Private Key / CSP	Asymmetric key used during TLS authentication	P-256 – 128	Private key	Internally generated per FIPS 186-4	N/A	TLS handshake
ECDSA Public Key Certificate / PSP	ECDSA Public Key Certificate issued by a CA	P-256 - 128	Public key	External	N/A	TLS handshake
Server Self-signed Certificate / PSP	ECDSA Public Key Certificate	P-256 - 128	Public key	Internal	N/A	TLS handshake
ECDSA Public Key Certificate (operator) / PSP	ECDSA Public Key Certificate issued by a CA	P-256 - 128	Public key	External	N/A	TLS handshake
CA Certificate / PSP	CA public key for certificate validation	P-256 - 128	Public key	External	N/A	mTLS
DRBG V / CSP	DRBG internal state	256 - 128	DRBG secret	Internal	N/A	DRBG
DRBG Key / CSP	DRBG internal state	256 - 128	DRBG secret	Internal	N/A	DRBG
Entropy Input / CSP	Bit string for seed generation	440 - 128	Entropy bit string	Internal	N/A	DRBG
DRBG Seed / CSP	Bit string to instantiate the DRBG	440 - 128	DRBG secret	Internal	N/A	DRBG
Password / CSP	Credential for operator authentication (Salted SHA2-256 protected)	Minimum of 8 characters	Authentication	N/A	N/A	SHA2-256
Hashed Password / CSP	Password hash	256	Authentication	Internal	N/A	SHA2-256
Operator Certificate / PSP	Client ECDSA public key certificate for mTLS	P-256 - 128	Public key	External	N/A	TLS handshake / Login
Access Token / CSP	Time-limited access token	P-256 - 128	Signature	Internal	N/A	ECDSA SigGen / ECDSA SigVer

Table 19: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
AES-GCM Key / CSP	N/A - N/A	RAM	Per connection	Per connection, tamper response, Reset/Zeroization service	Derived from TLS Master Secret
TLS Pre- master Secret / CSP	N/A - N/A	RAM	Per connection	Per connection, tamper response, Reset/Zeroization service	EC Diffie-Hellman Private Key, EC Diffie Hellman Public Key
TLS Master Secret / CSP	N/A - N/A	RAM	Per connection	Per connection, tamper response, Reset/Zeroization service	Derived from TLS Pre-master Secret
EC Diffie-Hellman Public Key / PSP	N/A - KAS-Out	RAM	Per connection	Per connection, tamper response, Reset/Zeroization service	EC Diffie-Hellman Private Key, EC Diffie-Hellman, TLS Pre-master Secret
EC Diffie-Hellman Public Key (operator) / PSP	KAS-In - N/A	RAM	Per connection	Per connection, tamper response, Reset/Zeroization service	TLS Pre-master Secret
EC Diffie-Hellman Private Key / CSP	N/A - N/A	RAM	Per connection	Per connection, tamper response, Reset/Zeroization service	EC Diffie-Hellman Public Key, EC Diffie-Hellman Public Key (operator), TLS Pre-master Secret
ECDSA Public Key / PSP	N/A - TLS Payload-Out	SRAM	Per connection	Per connection, tamper response, Reset/Zeroization service	ECDSA Private key
ECDSA Private Key / CSP	N/A - N/A	SRAM	Until replace by new ECDSA Key Pair by CO	Tamper response, Reset/Zeroization service	ECDSA Public key
ECDSA Public Key Certificate / PSP	Load Cert - TLS Handshake-Out	SRAM - RAM	Until replace by new ECDSA Key Pair by CO - Per connection	Tamper response, Reset/Zeroization service	ECDSA Public Key, ECDSA Private Key
Server Self-signed	N/A - TLS Handshake-	SRAM	Until replace by new ECDSA	Tamper response, Reset/Zeroization	ECDSA Public Key

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Certificate / PSP	Out		Key Pair by CO	service	
ECDSA Public Key Certificate (operator) / PSP	TLS Handshake-In - N/A	RAM	N/A	Per connection, tamper response, Reset/Zeroization service	CA Certificate
CA Certificate / PSP	Load Cert - N/A	SRAM	N/A	Tamper response, Reset/Zeroization service	Used to verify the trusted chain of certificate
DRBG V / CSP	N/A / N/A	RAM	Periodically updated	Reboot	DRBG Seed
DRBG Key / CSP	N/A / N/A	RAM	Periodically updated	Reboot	DRBG Seed
Entropy Input	N/A / N/A	RAM	DRBG reseed	Automatic at end of function call	DRBG Seed
DRBG Seed / CSP	N/A / N/A	RAM	DRBG reseed	Automatic at end of function call	Entropy Input
Password / CSP	TLS Payload-In - N/A	SRAM	Per connection	Per connection, tamper response, Reset/Zeroization service	N/A
Hashed Password / CSP	N/A – N/A	RAM	Per connection	Per connection, tamper response, Reset/Zeroization service	Password
Operator Certificate / PSP	KAS-In - N/A	RAM	Per connection	Per connection, tamper response, Reset/Zeroization service	N/A
Access Token / CSP	Token-In - Token-Out	RAM	Per connection	Per connection, tamper response, Reset/Zeroization service	ECDSA Public Key - ECDSA Private Key

Table 20: SSP Table 2

10 Self-Tests

10.1 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.

Algorithm or Test	Test Properties	Test Method	Type	Indicator	Details
ECDSA	P-256	Signature Verification	Software Integrity	SEC LED blinking	Signature Verification

Table 21: Pre-Operational Self-Tests

10.2 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.

The following table summarizes the content of the previous subsections:

Algorithm or Test	Test Properties	Test Method	Type	Indicator	Details	Condition
AES-ECB	128, 256	KAT	CAST	LED signal	Encrypt / Decrypt	Run during power-up
AES-GCM	128, 256	KAT	CAST	LED signal	Encrypt / Decrypt	Run during power-up
HMAC	SHA2-256, SHA2-384	KAT	CAST	LED signal	Message Authentication Code	Run during power-up
SHS	SHA2-256, SHA2-384	KAT	CAST	LED signal	Message Digest	Run during power-up
SHS	SHA3-256	KAT	CAST	LED signal	ENT conditioner	Run during power-up
ECDSA	P-256	KAT	CAST	LED signal	Sign / Verify	Run during power-up
KAS-ECC-SSC	P-256	KAT	CAST	LED signal	Shared Secret Computation	Run during power-up
TLSv1.3 KDF		KAT	CAST	LED signal	Key Derivation	Run during power-up
DRBG	HMAC_DRBG, Instantiate, Reseed and Generate	KAT	CAST	LED signal	Random Bit Generation	Run during power-up
ECDSA	P-256	PCT	CPCT	LED signal	Sign / Verify	Key Pair Generation
KAS-ECC-SSC	P-256	PCT	CPCT	LED signal	SP 800-56Arev3 assurance checks	Shared Secret Computation
ECDSA	P-256	Signature Verification	CFLT	LED signal	Digital Signature	Software update signature verification
ENT	APT, RCT and Lag health tests		CCFT	LED signal	SP 800-90B Health tests for Entropy Sources	Run during power-up (on 1,024 samples) and runtime health tests

Table 22: Conditional Self-Tests

10.3 Periodic Self-Tests

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

State 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 Maintenance Requirements

There are no maintenance requirements or maintenance role.

11.5 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.

13 Acronyms

AES	Advance Encryption System
ASCII	American Standard Code for Information Interchange
CA	Certificate Authority
CAST	Cryptographic Algorithm Self-test
CAVP	Cryptographic Algorithm Validation Program

CCFT	Conditional Critical Function Test
CDI	Communication Devices, Inc.
CFLT	Conditional Firmware Load Test
CMVP	Cryptographic Module Validation Program
CPCT	Conditional Pair-Wise Consistency Test
CO	Crypto Officer
CSR	Certificate Signing Request
DH	Diffie-Hellman
DRAM	Dynamic Random Access Memory
EC	Elliptical Curve
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)
	Data Set Ready
	TxD Transmit Data
	RxD Received Data
Flash	Flash Solid State Memory
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
PCM	Power Control Module
RM	Rack Mounted
RNG	Random Number Generator
SRAM	Static Random Access Memory
SA	Stand Alone
VAC	Voltage Alternating Current
VDC	Voltage Direct Current