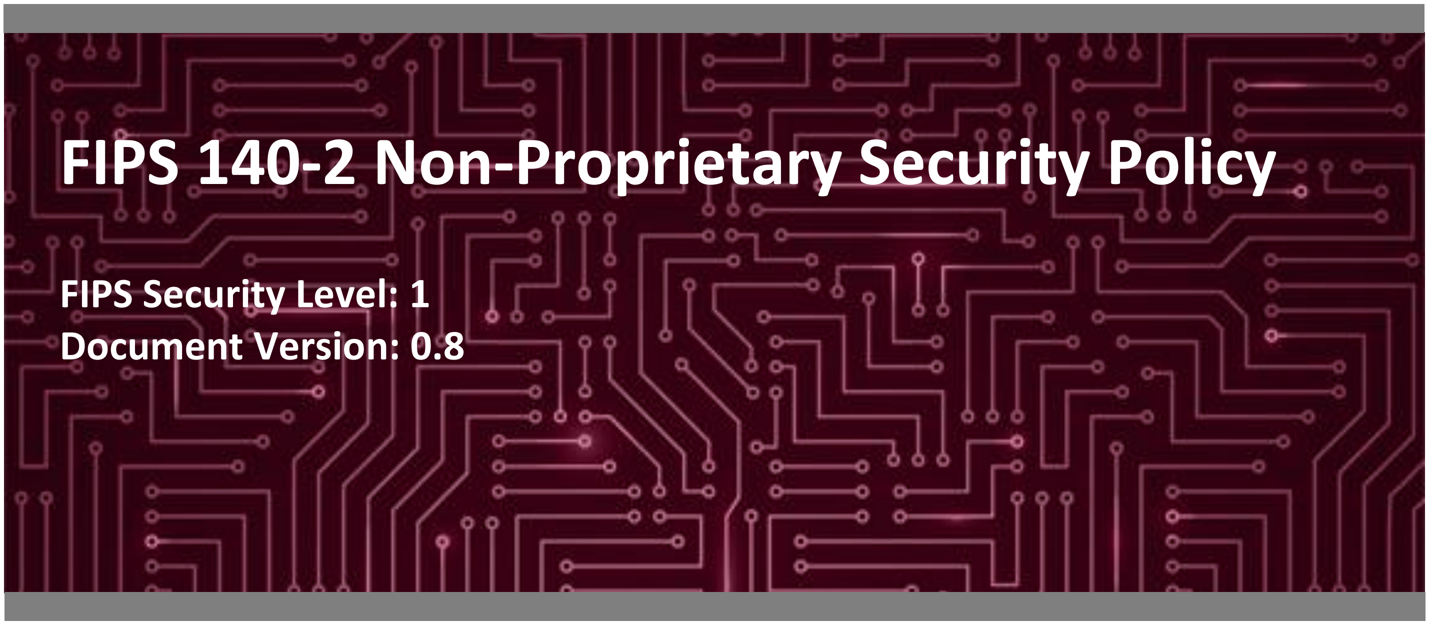
Certes Networks, Inc.

Certes Enforcement Points

Hardware Models: CEP220, CEP250, CEP300, CEP420, CEP520
Firmware Version: CEP v5.3



FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 1
Document Version: 0.8

Prepared for:

Certes Networks, Inc.
300 Corporate Center Drive, Suite 140
Pittsburgh, PA 15108
United States of America

Phone: +1 412 262 2571
www.certesnetworks.com

Prepared by:

Corsec Security, Inc.
13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

Phone: +1 703 267 6050
www.corsec.com

Table of Contents

List of Tables

List of Figures

1. Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Certes Enforcement Points (CEP) from Certes Networks, Inc. (Certes). This Security Policy describes how the CEPs meet the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S.[1] and Canadian government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) and the Communications Security Establishment (CSE) Cryptographic Module Validation Program (CMVP) website at http://csrc.nist.gov/groups/STM/cmvp.

This document also describes how to run the module in a secure FIPS-Approved mode of operation. This policy was prepared as part of the Level 1 FIPS 140-2 validation of the module. The CEPs are referred to in this document as the module or modules.

1.2 References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The Certes website (http://www.certesnetworks.com) contains information on the full line of products from Certes.
- The CMVP website (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm) contains contact information for individuals responsible for answering technical or sales-related questions for the module.

1.3 Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence
- Finite State Model
- Submission Summary
- Other supporting documentation as additional references

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to Certes. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Submission Package is proprietary to Certes and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Certes.

[1] U.S. – United States

2. Certes Enforcement Points

2.1 Overview

CEPs are purpose-built encryption appliances that provide multi-layer data protection and application segmentation. Running Certes' CEP v5.3 firmware, CEP appliances provide Ethernet frame encryption for Layer 2 networks, IPsec[2] encryption for Layer 3 networks, and data payload encryption for Layer 4 MPLS[3] networks. CEPs operate transparently to the network infrastructure, which ensures all data is encrypted without impacting network performance.

The CEP interfaces with network equipment through two data ports: the local port and the remote port. Unencrypted traffic that originates from a trusted, local network is received on the local port, where the CEP applies security processing. Encrypted traffic is sent from the remote port to an untrusted network, such as the Internet. At the opposite endpoint, the process is reversed. Encrypted traffic is received on the CEP remote port, where it is decrypted and sent from the local port to the destination. The decrypted traffic is sent from the local port to the destination. Encryption policies use IP[4] addresses, protocol IDs[5], or VLAN[6] tags to identify and apply security processing to network traffic. CEPs secure network traffic using 256-bit AES[7]-GCM[8] and AES-CBC[9] for encryption, as well as SHA[10]-2 for message integrity and authentication.

CEPs provide two types of ports that provide operator access to the module's management interfaces: Management Ports and Console Ports. Management Ports are GbE[11] ports, while Console Ports are serial ports. These ports allow access to the following interface mechanisms:

- CryptoFlow Net Creator (CFNC) – The CFNC is an external web-based management application that runs on a separate server within a connected network. Management is accomplished through the use of XML-RPC12, providing centralized key, policy, and device management for all CEPs in the network as well as logging and audit capabilities. This management traffic occurs via TLS session over a Management Port.

- Command Line Interface (CLI) – The CLI is typically used to manage a standalone CEP pair or to perform initial setup and diagnostics. The CLI is accessed locally via direct attachment to a Console Port or remotely via Secure Shell (SSH) session over a Management Port.

- SNMP – CEPs use the SNMPv3 protocol for remote management and to obtain network statistics. The SNMP interface is accessed over a Management Port.

[2] IPsec – Internet Protocol Security
[3] MPLS – Multiprotocol Label Switching
[4] IP – Internet Protocol
[5] ID – Identifier
[6] VLAN – Virtual Local Area Network
[7] AES – Advanced Encryption Standard
[8] GCM – Galois Counter Mode
[9] CBC – Cipher block chaining
[10] SHA – Secure Hash Algorithm
[11] GbE – Gigabit Ethernet
[12] XML-RPC – eXtensible Markup Language – Remote Procedure Call

The CEP220 and CEP250 provide up to 200 Mbps[13] performance in a small form factor enclosure as shown in Figure 1.

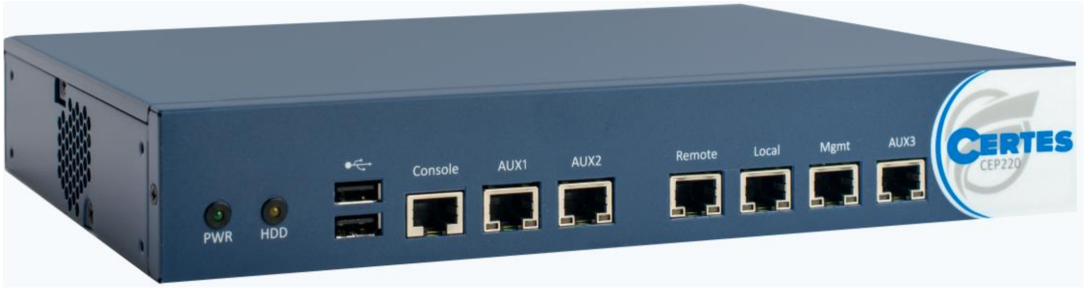


Figure 1 – CEP220/CEP250

The CEP300 provides up to 1 Gbps[14] performance in a 1U[15] rack-mountable enclosure, as shown in Figure 2**.**

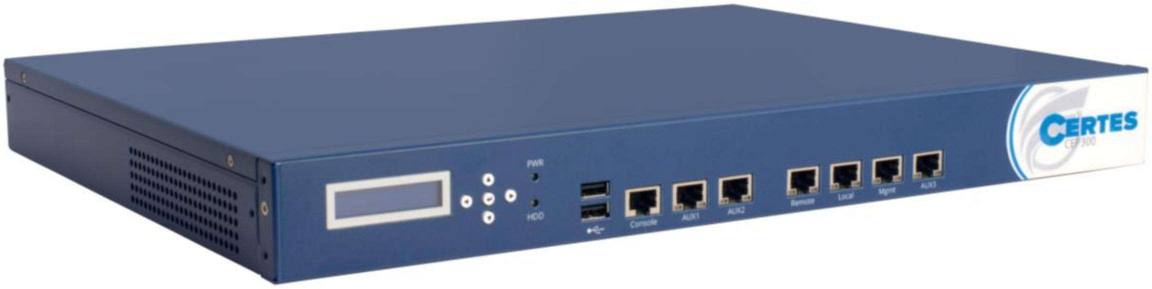


Figure 2 – CEP300

The CEP420 provides up to 1 Gbps performance in a 1U rack-mountable enclosure but with additional network interfaces, as shown in Figure 3.

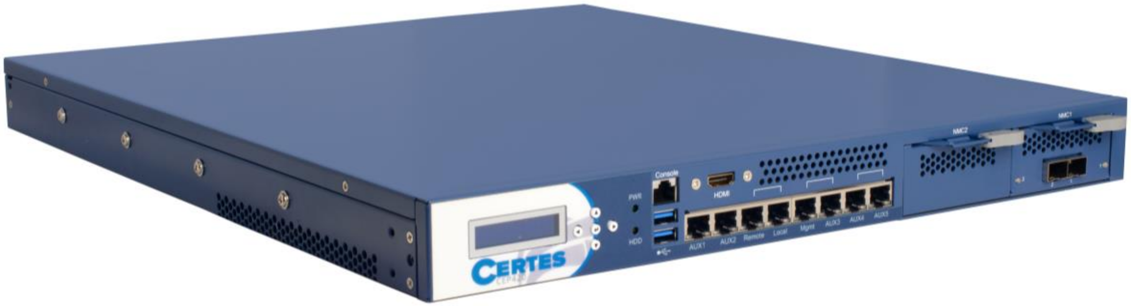


Figure 3 – CEP420

The CEP520 provides up to 10 Gbps performance in a 1U rack-mountable enclosure, as shown in Figure 4.

[13] Mbps – Megabits per second
[14] Gbps – Gigabits per second
[15] U – Rack Unit

Figure 4 – CEP520

The CEPs are validated at the FIPS 140-2 Section levels shown in Table 1.

Table 1 – Security Level per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	1
4	Finite State Model	1
5	Physical Security	1
6	Operational Environment	N/A
7	Cryptographic Key Management	1
8	EMI/EMC[16]	1
9	Self-tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A

2.2 Module Specification

The CEP is a hardware module with a multiple-chip standalone embodiment. The overall security level of the module is 1. The cryptographic boundary is defined by the physical enclosure of the CEP and includes all internal hardware as well as the CEP v5.3 firmware.

The diagram and cryptographic boundary for each model is depicted in Figure 5, Figure 6, Figure 7, and Figure 8. The following undefined acronyms appear in Figure 5 below:

- DDR – Double Data Rate
- HWM – Hardware Monitor
- LAN – Local Area Network
- LED – Light Emitting Diode

[16] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility

- mSATA – Mini Serial Advanced Technology Attachment
- PCIe – Peripheral Component Interconnect Express
- PSU – Power Supply
- RAM – Random Access Memory
- SOC – System On Chip
- SSD – Solid State Drive
- USB – Universal Serial Bus

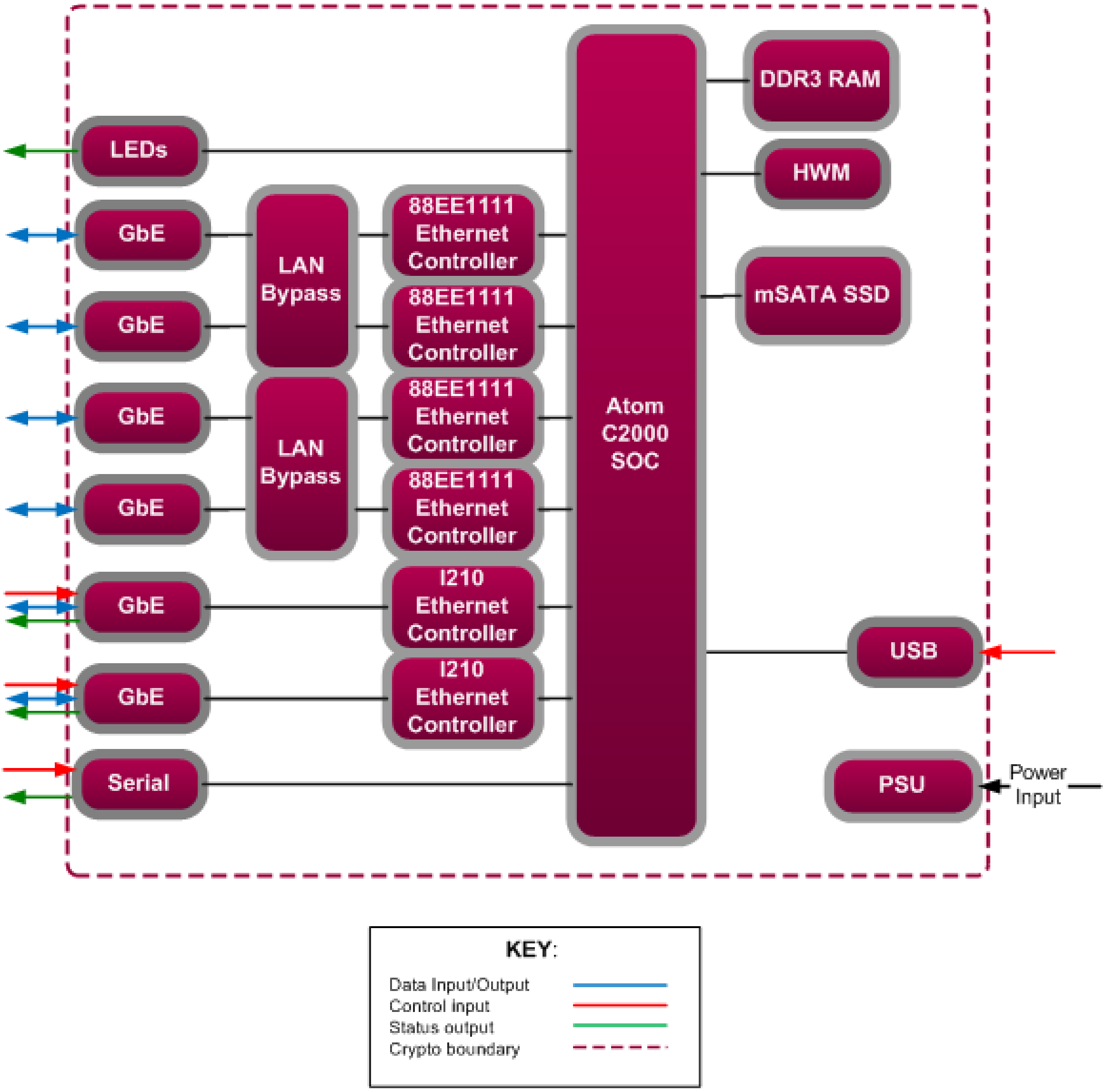


Figure 5 – CEP220/CEP250 Block Diagram

The following undefined acronyms appear in Figure 6 below:

- LCD – Liquid Crystal Display

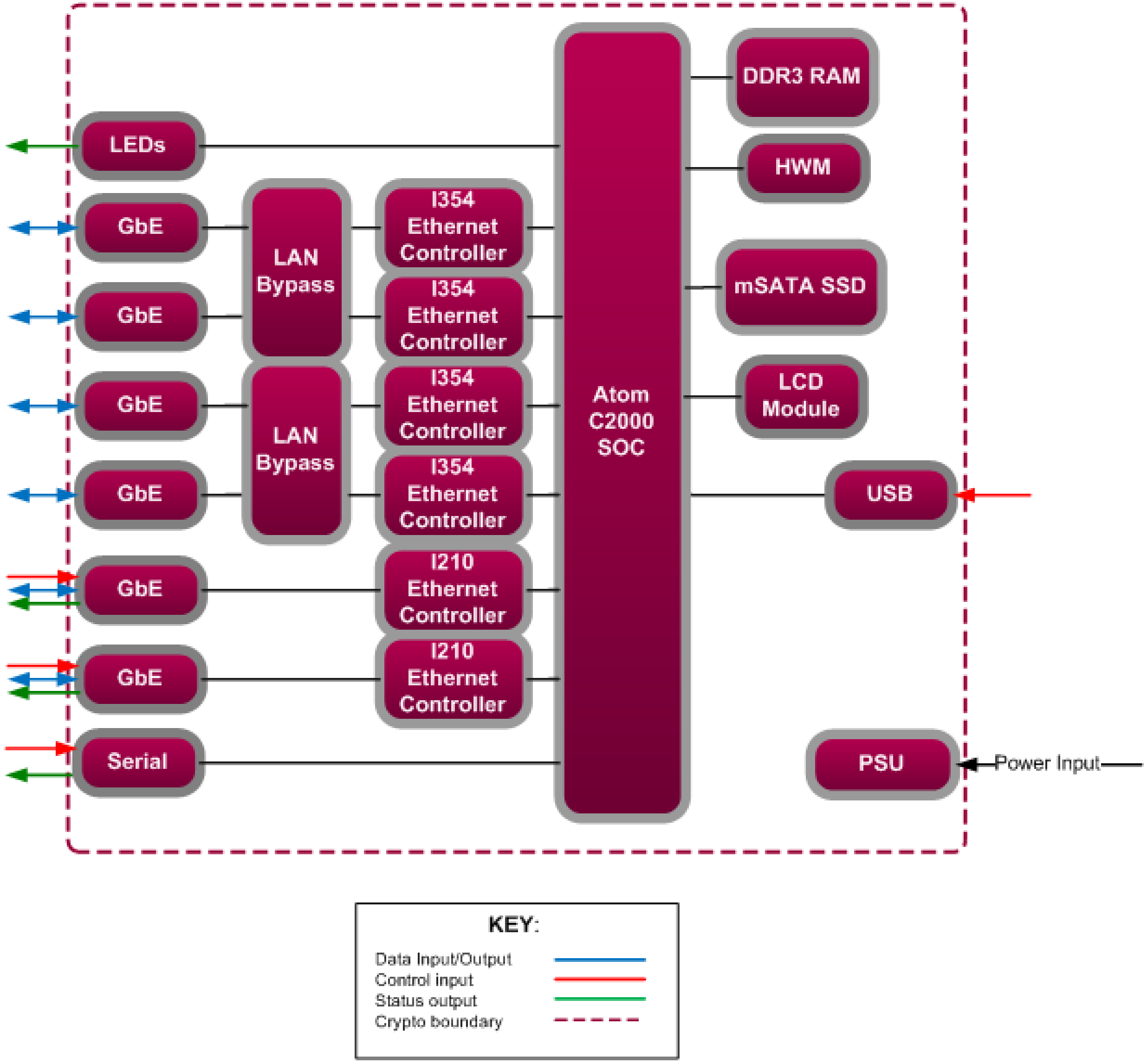


Figure 6 – CEP300 Block Diagram

The following undefined acronyms appear in Figure 7 below:

- BMC – Baseboard Management Controller
- EEPROM – Electrically Erasable Programmable Read-Only Memory
- PCH – Platform Controller Hub
- SATA – Serial Advanced Technology Attachment
- TPM – Trusted Platform Module

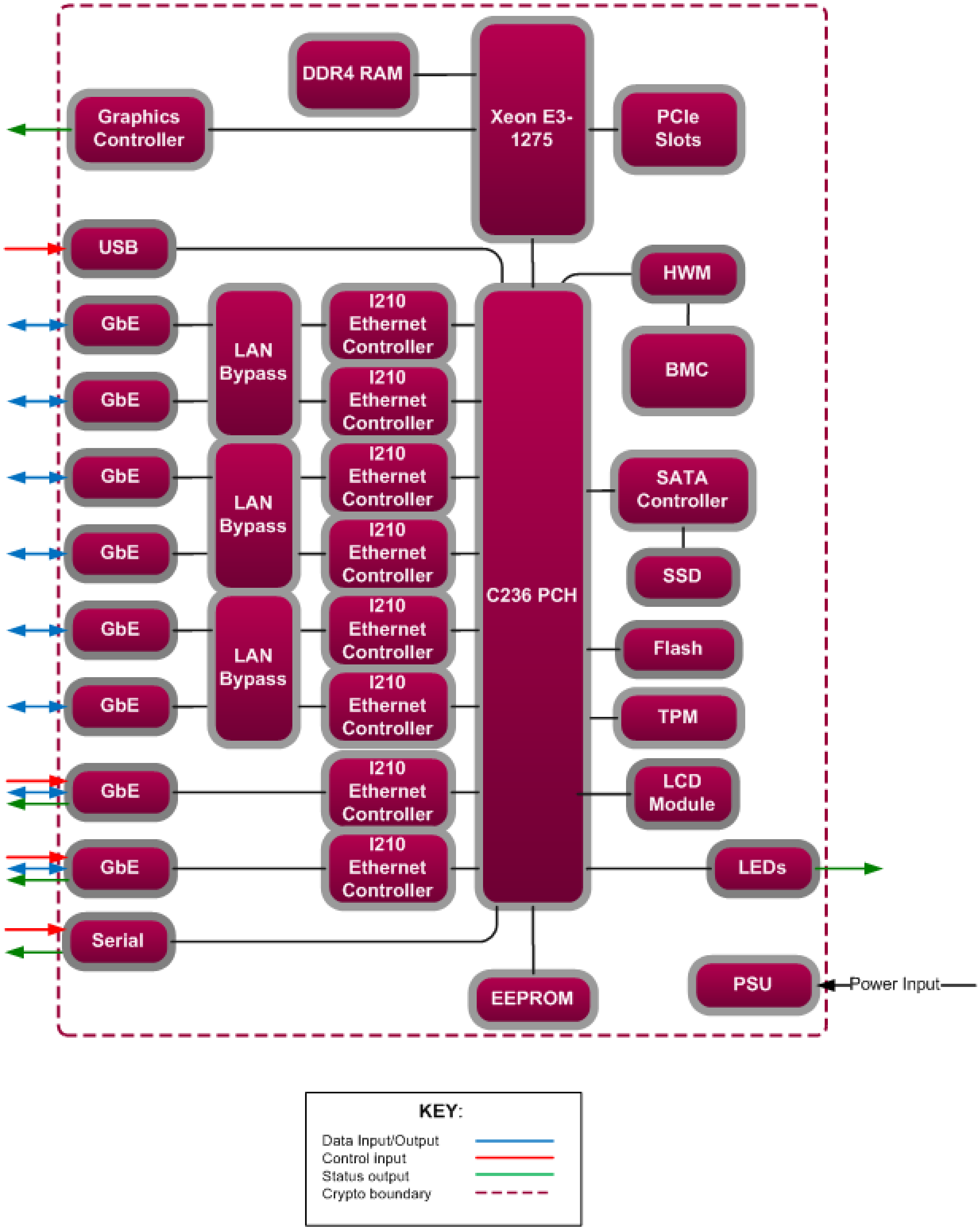


Figure 7 – CEP420 Block Diagram

The following undefined acronyms appear in Figure 8 below:

- SFP – Small Form Factor Pluggable

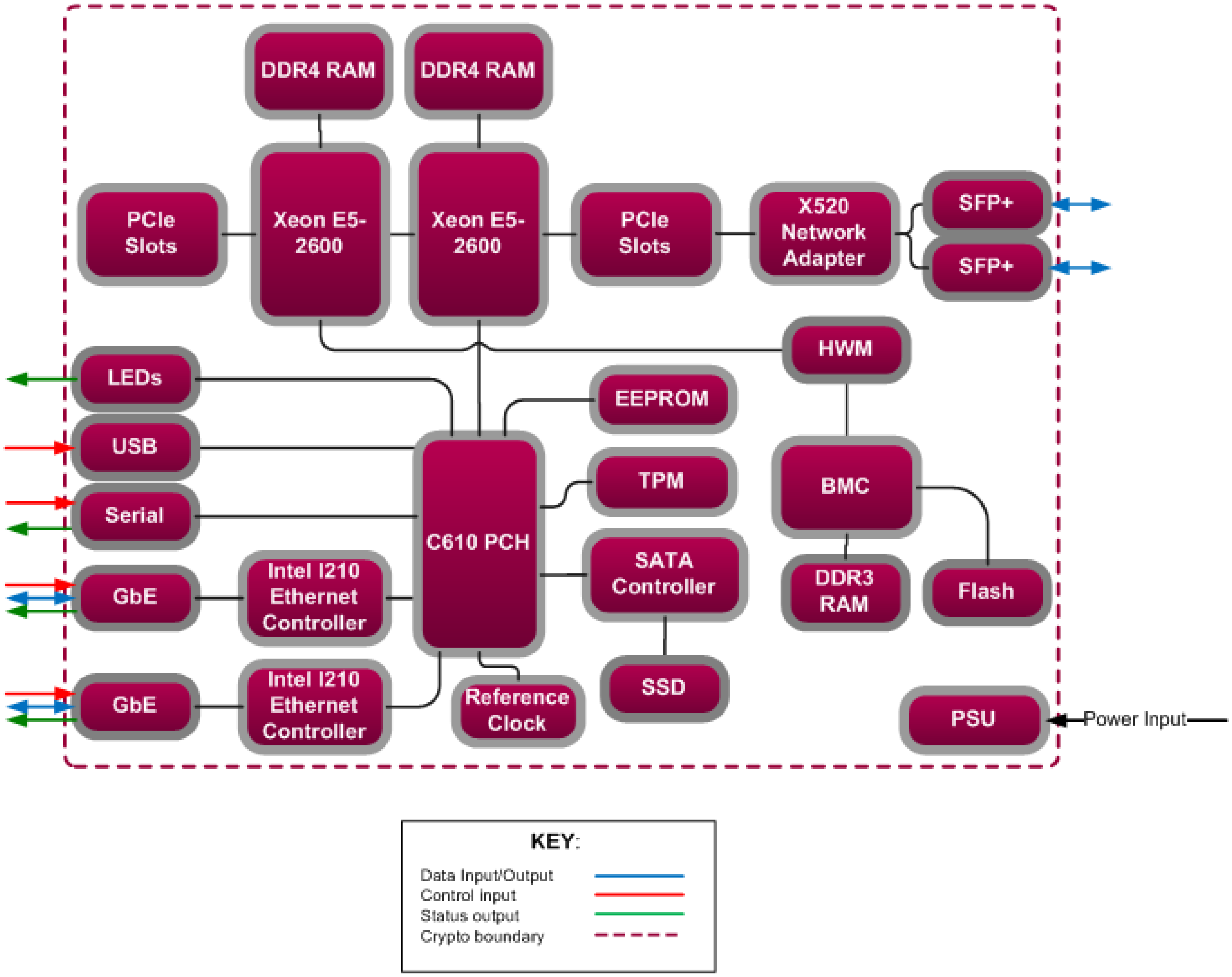


Figure 8 – CEP520 Block Diagram

Figure 9 below depicts the logical diagram of the CEP firmware.

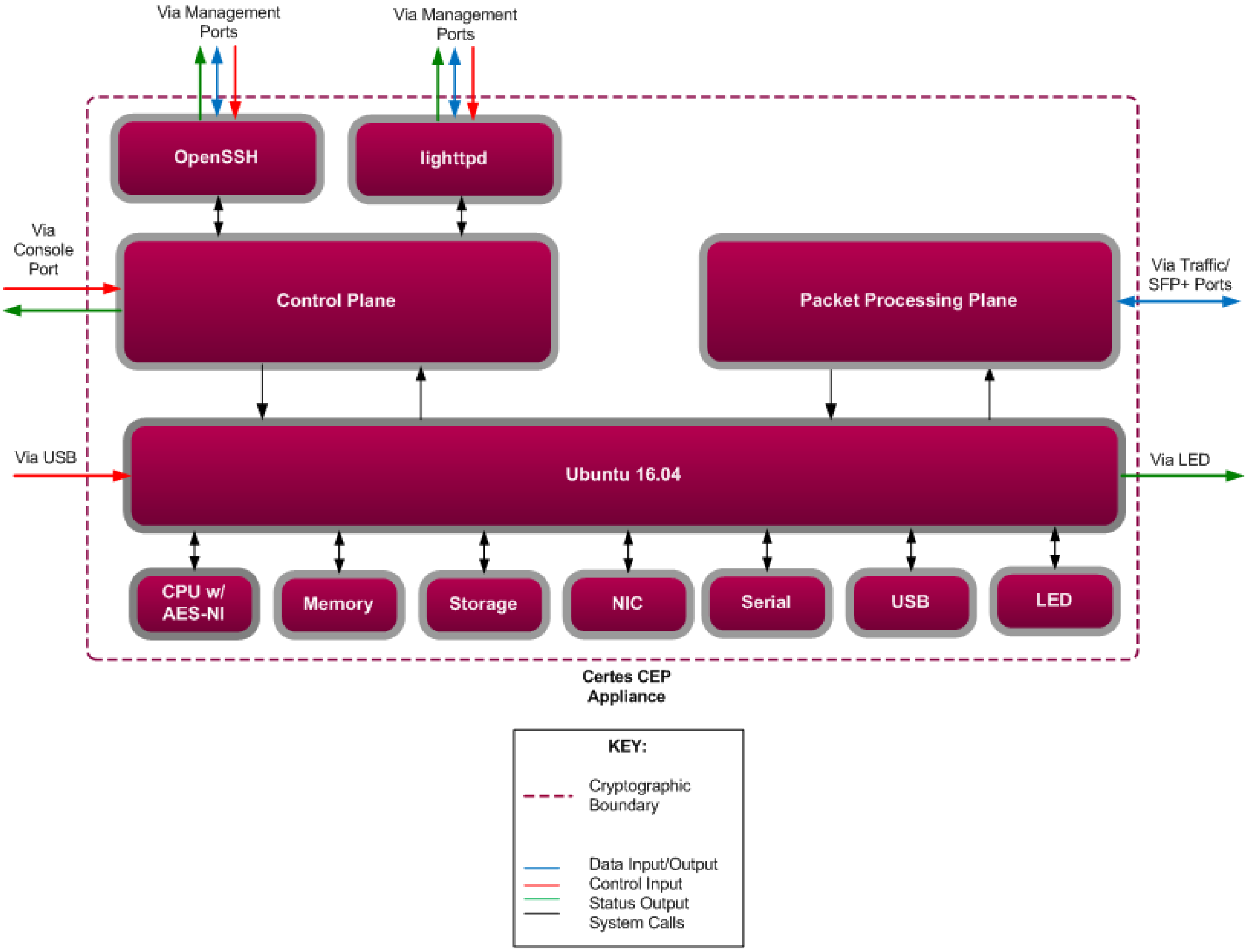


Figure 9 – Logical Block Diagram of CEP Appliance

The module implements the FIPS-Approved cryptographic algorithms listed in Table 2.

Table 2 – FIPS-Approved Algorithm Implementations

CAVP[17] Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli	Use
5338	AES	FIPS PUB[18] 197, NIST SP[19] 800-38A	CBC	128, 256	Data encryption/decryption
			ECB[20]	128, 192, 256	Data encryption/decryption ECB mode used in support of CTR[21].
			CFB128[22]	128	Data encryption/decryption
			CTR	128, 192, 256	Data encryption/decryption
		FIPS PUB 197, NIST SP 800-38D	GCM	128, 256	Data encryption/decryption and authentication
		FIPS PUB 197, NIST SP 800-38D	CMAC[23]	256	Generation and verification
Vendor Affirmation	CKG[24]	NIST SP 800-133	-	-	Key generation *Symmetric keys and generated seeds are produced using unmodified output from the Approved DRBG.*
1800	CVL	NIST SP 800-56A	ECC CDH[25]	P-224 P-256, P-384, P-521	Shared secret computation *P-224 curve used only for ECC CDH known answer test.*
1827	CVL[26]	NIST SP 800-135rev1	TLSv1.2 with SHA-256, SHA-384, SHA-512	-	Key derivation *No parts of the TLS protocol, other than the KDF, have been tested by the CAVP and CMVP.*
1828	CVL	NIST SP 800-135rev1	SSHv2 with SHA-1, SHA-256, SHA-384, SHA-512	-	Key derivation *No parts of the SSH protocol, other than the KDF, have been tested by the CAVP and CMVP.*

[17] CAVP – Cryptographic Algorithm Validation Program
[18] PUB – Publication
[19] SP – Special Publication
[20] ECB – Electronic Codebook
[21] CTR – Counter
[22] CFB – Cipher Feedback
[23] CMAC – Cipher-based Message Authentication Code
[24] CKG – Cryptographic Key Generation
[25] ECC DH – Elliptic Curve Cryptography Co-factor Diffie-Hellman
[26] CVL – Component Validation List

CAVP[17] Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli	Use
1829	CVL	NIST SP 800-135rev1	SNMPv3[27] with SHA-1, SHA-256, SHA-384, SHA-512	-	Key derivation *No parts of the SNMPv3 protocol, other than the KDF, have been tested by the CAVP and CMVP.*
2061	DRBG[28]	NIST SP 800-90A	CTR	256-bits	Deterministic random bit generation with derivation function
1402	ECDSA[29]	FIPS PUB 186-4	PKG	P-224 P-256, P-384, P-521	Key pair generation *P-224 curve used only for ECDSA pairwise consistency test.*
			SigGen, SigVer	P-224, P-256, P-384, P-521	Digital signature generation and verification *P-224 curve used only for ECDSA pairwise consistency test.*
3535	HMAC[30]	FIPS PUB 198-1	HMAC SHA-1, HMAC SHA-256, HMAC SHA-384, HMAC SHA-512	160, 256, 384, 512	Message authentication
193	KBKDF[31]	NIST SP 800-108	Counter mode with AES-CMAC	-	Key derivation
4289	SHS[32]	FIPS PUB 180-4	SHA-1, SHA-256, SHA-384, SHA-512	-	Message digest *SHA-1 is only used for SSH and SNMP protocols.*

The module implements the non-Approved but allowed algorithms shown in Table 3.

Table 3 – Allowed Algorithm Implementations

Algorithm	Caveat	Use
EC Diffie-Hellman (CVL Cert. #1800)	Key establishment methodology provides between 128 and 256 bits of encryption strength	Key agreement

[27] SNMP – Simple Network Management Protocol
[28] DBRG – Deterministic Random Bit Generator
[29] ECDSA – Elliptic Curve Digital Signature Algorithm
[30] HMAC – (keyed-) Hashed Message Authentication Code
[31] KBKDF – Key-based Key Derivation Function
[32] SHS – Secure Hash Standard

Algorithm	Caveat	Use
NDRNG[33]	The module generates cryptographic keys whose strengths are modified by the available entropy.	The internal hardware-based NDRNG used to seed the Approved SP 800-90A CTR_DRBG. The module generates a minimum of 256 bits of entropy for key generation.

2.3 Module Interfaces

The CEP220 and CEP250 contain the physical ports and interfaces shown in Figure 10 and Figure 11 below.

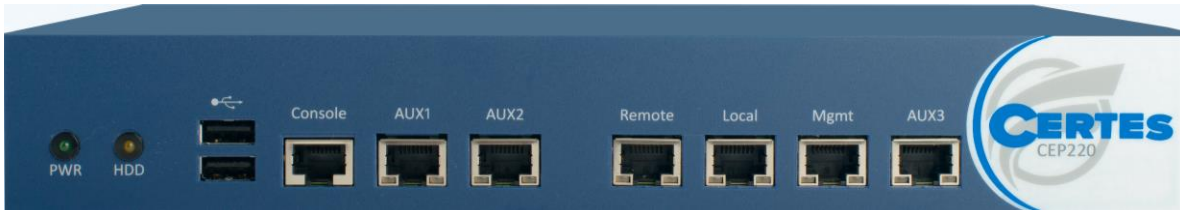


Figure 10 – CEP220/CEP250 Ports and Interfaces (Front)

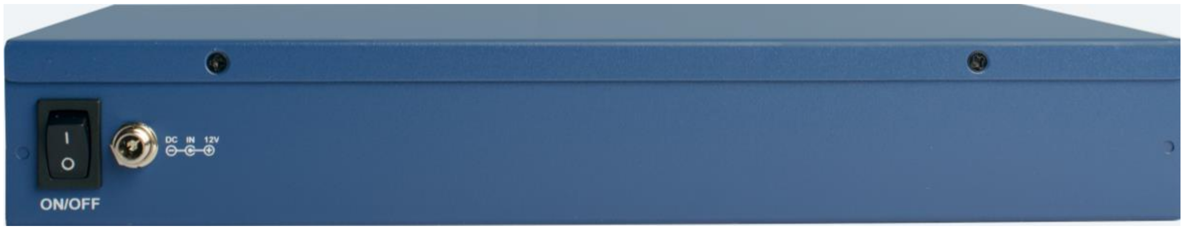


Figure 11 – CEP220/CEP250 Ports and Interfaces (Rear)

The CEP300 contains the physical ports and interfaces shown in Figure 12 and Figure 13 below.

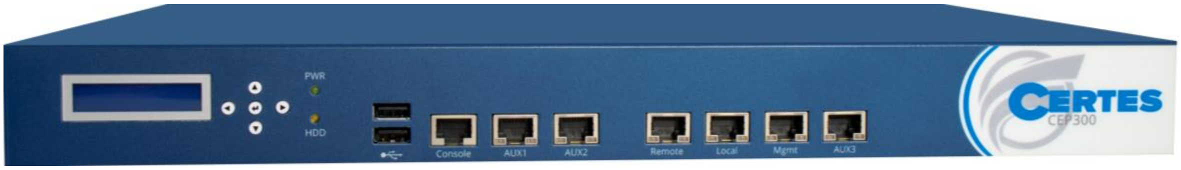


Figure 12 – CEP300 Ports and Interfaces (Front)

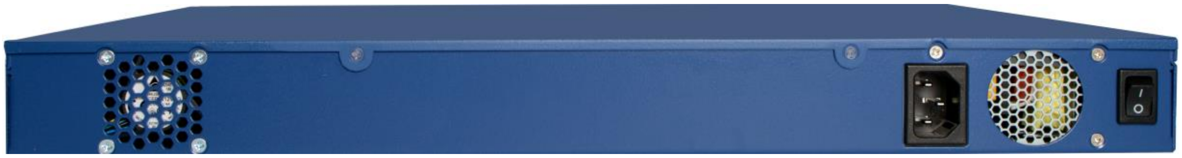


Figure 13 – CEP300 Ports and Interfaces (Rear)

[33] NDRNG – Non-Deterministic Random Number Generator

The CEP420 contains the ports and interfaces shown in Figure 14 and Figure 15 below.

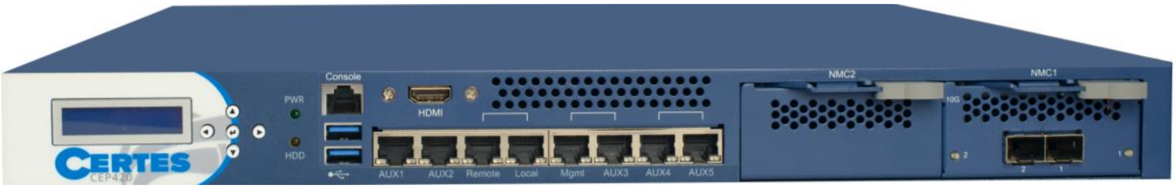


Figure 14 – CEP420 Ports and Interfaces (Front)

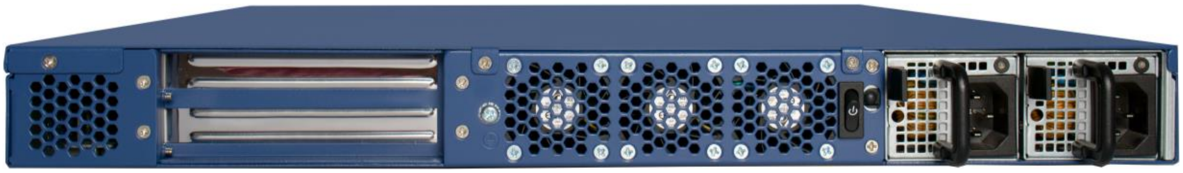


Figure 15 – CEP420 Ports and Interfaces (Rear)

The CEP520 contains the ports and interfaces shown in Figure 16 and Figure 17 below.

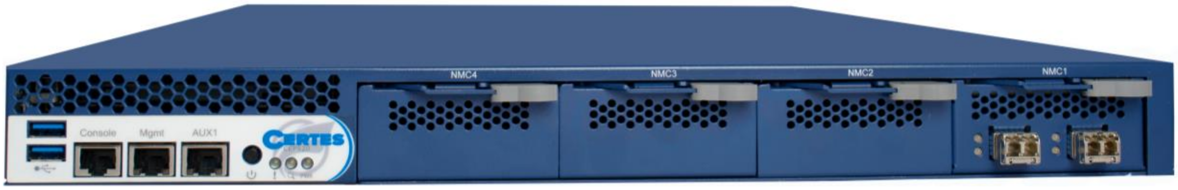


Figure 16 – CEP520 Ports and Interfaces (Front)

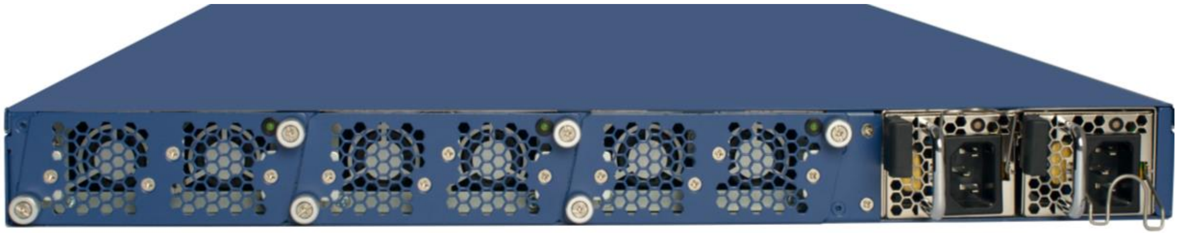


Figure 17 – CEP520 Ports and Interfaces (Rear)

The physical interfaces for the CEP are mapped to the FIPS 140-2 logical interfaces in Table 4.

Table 4 – Mapping of FIPS 140-2 Logical Interfaces to CEP Interfaces

Physical Port/Interface	Quantity	FIPS 140-2 Interfaces
CEP220/CEP250		
Power LED	1	Status Output
HDD LED	1	N/A
USB Ports	2	N/A

Physical Port/Interface	Quantity	FIPS 140-2 Interfaces
Console Port	1	Control Input, Status Output, Data Input, Data Output
Management Port	1	Control Input, Status Output, Data Input, Data Output
Traffic Ports (Remote/Local)	2	Data Input, Data Output
Auxiliary Ports	3	N/A (Disabled in FIPS-Approved mode)
Power On/Off Switch	1	Control Input
CEP300		
LCD Panel/Buttons	1	N/A
Power LED	1	Status Output
HDD LED	1	N/A
USB Ports	2	N/A
Console Port	1	Control Input, Status Output, Data Input, Data Output
Management Port	1	Control Input, Status Output, Data Input, Data Output
Traffic Ports (Remote/Local)	2	Data Input, Data Output
Auxiliary Ports	3	N/A (Disabled in FIPS-Approved mode)
Power On/Off Switch	1	Control Input
CEP420		
LCD Panel/Buttons	1	N/A
Power LED	1	Status Output
HDD LED	1	N/A
Console Port	1	Control Input, Status Output, Data Input, Data Output
USB Ports	2	N/A
HDMI Port	1	Status Output
Management Port	1	Control Input, Status Output, Data Input, Data Output
Traffic Ports (Remote/Local)	2	Data Input, Data Output
Auxiliary Ports	5	N/A (Disabled in FIPS-Approved Mode)
Power On/Off Switch	1	Control Input
CEP520		
USB Ports	2	N/A
Console Port	1	Control Input, Status Output, Data Input, Data Output
Management Port	1	Control Input, Status Output, Data Input, Data Output
Auxiliary Port	1	N/A (Disabled in FIPS-Approved Mode)
Locate LED	1	N/A
Alert LED	1	N/A
Power LED	1	Status Output
SFP+ Ports	2	Data Input, Data Output
Power Button	1	Control Input

2.4 Roles and Services

The following sections detail the roles and services provided by the module.

2.4.1 Roles

There are three roles supported by the module that operators may assume: Cryptographic Officer (CO) role, User role, and SNMP role. CO and User roles are assumed explicitly by means of authenticating with an account associated with a role. The SNMP role is assumed explicitly by establishing a SNMPv3 session with the correct authentication and privacy passwords.

2.4.1.1 Crypto Officer Role

The CO role maps to the "Administrator" and "CFNC Administrator" product roles. The "Administrator" role is used for accessing the module CLI via SSH (over the management port) or serial connection (via console port), while the "CFNC Administrator" role accesses the module via XML-RPC over TLS from the remote CFNC application (through the management port). Each CO has their own account with a username and password. The CO's account credentials are used to authenticate to the module. The CO can access all administrative services offered by the module, including user management, appliance configuration, and policy management. The full list of CO services can be found in Table 5 below and are denoted by 'C'.

2.4.1.2 User Role

The User role maps to the CEP "Ops" product role. The User role can also access the module's CLI via SSH (management port) or serial connection (console port); however, it only has a limited subset of commands available, which include initial appliance configuration, status reporting, and diagnostics. Each User has their own account with a username and password. The User's account credentials are used to authenticate to the module. The full list of User services can be found Table 5 below and are denoted by 'U'.

2.4.1.3 SNMP Role

The SNMP role maps to SNMP manager applications accessing the module via its management port. The SNMPv3 protocol is used for retrieving networking statistics and requires an authentication and privacy password. The full list of SNMP services can be found in Table 5 below and are denoted by 'S'.

2.4.1.4 Multiple Concurrent Operators

The module supports multiple concurrent operators. The module can support a Console Port CLI session along with multiple remote CLI sessions and multiple XML-RPC sessions on the Management Ports. Each session remains active (logged in) and secured until the operator logs out or is automatically logged out after the inactivity timer expires (default of 10 minutes). While multiple concurrent sessions are allowed, the system restricts processing to four simultaneous commands.

Any shared resources that may be accessed via any user interface are semaphore-protected so that no two 'write' operations can occur simultaneously.

2.4.2 Services

Descriptions of the services available to each role as well as CSP access are detailed in Table 5 below. Please note that the keys and CSPs listed in the table indicate the type of access required and that the following notations are used:

- R – Read: The CSP is read.
- W – Write: The CSP is established, generated or modified.
- X – Execute: The CSP is used within an Approved or Allowed security function or authentication mechanism.
- D – The CSP is zeroized.

Table 5 – Mapping of Module Services to Roles, CSPs, and Type of Access

Service	Role			Description	Input	Output	CSP and Type of Access
	C	U	S				
Authenticate	✓	✓		Authenticate to the module	Authentication credential (username and password)	Authentication result (success/fail)	Password – X
Manage Users	✓			Create, change, or delete Ops and Admin users	*user-add* *user-delete* *user-enable* *user-disable* *user-modify* XML-RPC command	Command response XML-RPC response code	None
Set Password Policy	✓			Define the password policy for Ops and Admin users	*password-enforcement* XML-RPC command	Command response XML-RPC response code	None
Change Password	✓			Change Ops and Admin passwords	*password*	Command response XML-RPC response code	Password – W
Change Own Password	✓	✓		Change password of the current user	*password*	Command response XML-RPC response code	Password – W
View Audit Log	✓			View the audit log information	*show audit-log* XML-RPC command	Command response XML-RPC response code	None
Zeroization	✓			Zeroize the CEP	*clear-policies* *filesystem-reset* XML-RPC command	Command response XML-RPC response code	All CSPs – D (filesystem-reset command) IPsec Session Key – D (*clear-policies* command will delete IPsec keys) IPsec Key Derivation Key – D (*clear-policies* command will delete IPsec keys)

Service	Role			Description	Input	Output	CSP and Type of Access
	C	U	S				
Perform Self-Tests	✓			Perform self-tests on-demand	*reboot* Power-cycle	Command response XML-RPC response code Module restarts	None
Show Status	✓	✓		Display status of the module	*show fips-status* *show spd* XML-RPC command	Command response XML-RPC response code	None
Configure Basic Settings	✓			Configure IP addresses, datetime, licensing, auto-negotiation and flow control settings	*ip* *ipv6* *date* *auto-neg* XML-RPC command	Command response XML-RPC response code	None
Configure Advanced Settings	✓			Configure CLI inactivity timer, loss of signal pass through settings	*cli-inactivity-timer* *tx-enable* XML-RPC command	Command response XML-RPC response code	None
Configure Layer 3 Settings	✓			Configure network interoperability and transparent mode for Layer 3 policies	*reassembly* *dfbit-ignore* *ipv6traffic* *dhcprelay* XML-RPC command	Command response XML-RPC response code	None
Shutdown	✓			Shutdown the module	*shutdown* XML-RPC command	Command response XML-RPC response code	All ephemeral CSPs – D
Reboot	✓	✓		Reboot the module	*reboot* XML-RPC command	Command response XML-RPC response code	All ephemeral CSPs – D
Configure Security Policies	✓			Configure the policy mode, enable or disable CFNC policy management	*policy-mode* XML-RPC command	Command response XML-RPC response code	None
Configure KD[34] Message	✓			Supply an IPsec KD Message for IPsec Session Key derivation	XML-RPC command	XML-RPC response code	IPsec KD Message – W
Firmware Maintenance	✓			Perform firmware upgrade or downgrade	*install* XML-RPC command	Command response XML-RPC response code	All CSPs except ECDSA keypairs – W Firmware Load Test Key – RX
Configure SNMP	✓			Configure SNMPv3 trap settings	*snmp-config* XML-RPC command	Command response XML-RPC response code	SNMP Authentication Password – W SNMP Encryption Password – W

[34] KD – Key Derivation

Service	Role			Description	Input	Output	CSP and Type of Access
	C	U	S				
Encrypt/Decrypt SNMP data			✓	Encrypt/decrypt SNMP data	Establish SNMP protocol session	SNMP session established	SNMP Encryption Key – RX SNMP Encryption Password – RX
Authenticate SNMP data			✓	Authenticate SNMP data	Establish SNMP protocol session	SNMP session established	SNMP Authentication Key - RX SNMP Authentication Password – RX
Manage Certificates/Keypairs	✓			Generate ECDSA keypairs, certificate signing requires, install certificates, or revert to self-signed certificate	XML-RPC command	Command response XML-RPC response code	ECDSA Private Key – RWX ECDSA Public Key – RWX DRBG Entropy Input String – RX DRBG Seed – RX DRBG Key Value – RX DRBG 'V' Value – RX
Establish SSH Session	✓	✓		Connect to module via SSH to enter CLI commands	Command to establish SSH session	SSH session established	ECDSA Private Key – RX ECDSA Public Key – RX ECC CDH Public Components – RX ECC CDH Private Components – RX SSH Encryption Key – RWX SSH Authentication Key – RWX SSH Shared Secret – RWX AES-GCM IV – RWX DRBG Entropy Input String – RX DRBG Seed – RX DRBG Key Value – RX DRBG 'V' Value – RX
Establish TLS Session	✓			Connect to module via TLS from CFNC	Command to establish TLS session	TLS session established	ECDSA Private Key – RX ECDSA Public Key – RX ECC CDH Public Components – RX ECC CDH Private Components – RX TLS Encryption Key – RWX TLS Authentication Key – RWX TLS Pre-master Secret – RWX TLS Master Secret - RWX AES-GCM IV – RWX DRBG Entropy Input String – RX DRBG Seed – RX DRBG Key Value – RX DRBG 'V' Value – RX

A complete listing of the module's available services can be found in the *Certes CEP User Guide, Version 5.3 REV A,* and the *Certes CryptoFlow Net Creator User Guide, Version 5.3 REV A.*

2.4.3 Additional Services

The module provides a limited number of services for which the operator is not required to assume an authorized role. Table 6 lists the services for which the operator is not required to assume an authorized role. None of the services listed in the table modify, disclose, or substitute cryptographic keys and CSPs, or otherwise affect the security of the module.

Table 6 – Additional Services

Service	Description	CSP and Type of Access
Transmit/receive network traffic	Send network data through the module	IPsec Session Key – RX IPsec Key Derivation Key – RX AES-GCM IV – RX

2.4.4 Alternating Bypass Capability

The module implements an alternating bypass capability in which network traffic is passed unencrypted if a packet matches a bypass policy. Two steps are required in order to enter the bypass state. The first step is the pepd process receiving the XML-RPC message as a result of a user-initiated (CLI or CFNC) event. The second is that the policy is pushed to the ipsec daemon for application to the packet processing engine. In addition, the module must pass the conditional bypass test. If the bypass test is successful, the bypass operation is allowed. If the test fails, the module enters a critical error state and the packet is dropped.

2.5 Physical Security

The CEP is a multiple-chip standalone cryptographic module. The module consists of production-grade components that are micro-coated using industry-standard passivation techniques.

2.6 Operational Environment

The module employs a non-modifiable operating environment. The CEP firmware is executed by the module's processor as indicated below:

- CEP220 (Intel® Atom Processor C Series processor)
- CEP250 (Intel® Atom Processor C Series processor)
- CEP300 (Intel® Atom Processor C Series processor)
- CEP420 (Intel® Xeon® Processor E3 v5 Family processor)
- CEP520 (dual Intel Xeon® Processor E5 v4 Family processor)

The module runs a customized operating system based on Ubuntu 16.04, which cannot be modified and does not provide a general-purpose computing environment.

2.7 Cryptographic Key Management

The module supports the CSPs listed in Table 7.

Table 7 – List of Cryptographic Keys, Cryptographic Key Components, and CSPs

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
TLS Pre-Master Secret	Pre-master secret for TLS	Established using ECC CDH key agreement	Never output from module	Plaintext in volatile RAM	End TLS session, Power cycle	Derivation of TLS Master Secret
TLS Master Secret	Master secret for TLS	Derived internally from TLS Pre-Master Secret established using TLS KDF	Never output from module	Plaintext in volatile RAM	End TLS session, Power cycle	Derivation of TLS Authentication Key and TLS Encryption Key
TLS Authentication Key	HMAC-SHA-256, HMAC-SHA-384, or AES-GCM (for GCM-based cipher suites only) key	Derived internally from TLS Pre-Master Secret established using TLS KDF	Never output from module	Plaintext in volatile RAM	End TLS session, Power cycle	Message authentication within the TLS protocol
TLS Encryption Key	AES (CBC or GCM) key	Derived internally from TLS Pre-Master Secret established using TLS KDF	Never output from module	Plaintext in volatile RAM	End TLS session, Power cycle	Encryption/Decryption within the TLS protocol
SSH Shared Secret	Shared secret for SSH	Established using ECC CDH key agreement	Never output from module	Plaintext in volatile RAM	End SSH session, Power cycle	Derivation of SSH Encryption Key and SSH Authentication Key
SSH Authentication Key	HMAC SHA-256 HMAC SHA-512, or AES-GCM (for GCM-based cipher suites only) key	Derived internally from SSH Shared Secret using SSH KDF	Never output from module	Plaintext in volatile RAM	End SSH session, Power cycle	Message authentication within the SSH protocol
SSH Encryption Key	AES (CTR or GCM) key	Derived internally from SSH Shared Secret using SSH KDF	Never output from module	Plaintext in volatile RAM	End SSH session, Power cycle	Encryption/Decryption within the SSH protocol
AES GCM IV[35]	96-bit IV	**G**enerated internally using an SP800-90A approved DRBG	Never output from module	Plaintext in volatile RAM	End session, Power cycle	IV input to AES-GCM function.
IPsec KD Message	256-bit KBKDF input value	Generated externally and input from CFNC over TLS in ciphertext	Never output from module	Plaintext in non-volatile Flash	Factory reset, Filesystem reset, Clear policies	Input value for derivation of IPsec Session key

[35] IV – Initialization Vector

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
IPsec Key Derivation Key	KBKDF key derivation key (256-bit AES-CMAC key)	Generated externally and input from CFNC over TLS in ciphertext	Never output from module	Plaintext non-volatile Flash	Factory reset, Filesystem reset, Clear policies	Key derivation key for derivation of IPsec Session key
IPsec Session Key	256-bit AES CMAC key	Derived internally using KBKDF	Never output from module	Plaintext in volatile RAM	Rekey, Power cycle	Encryption/decryption and message authentication within the IPsec protocol
ECDSA Private Key	P-256, P-384, P-521	Generated internally according to SP 800-133 CKG using SP 800-90A DRBG	Never output from module	Plaintext in non-volatile Flash	Factory reset, Filesystem reset	Digital signatures within TLS and SSH protocols
ECDSA Public Key	P-256, P-384, P-521	Generated internally according to SP 800-133 CKG using SP 800-90A DRBG	Output from the Management Port in plaintext	Plaintext in non-volatile Flash	Factory reset, Filesystem reset	Digital signatures within TLS and SSH protocols
ECC CDH Private Component	P-256, P-384, P-521	Generated internally according to SP 800-133 CKG using SP 800-90A DRBG	Never output from module	Plaintext in non-volatile Flash	Factory reset, Filesystem reset	Key agreement within TLS and SSH protocols
ECC CDH Public Component	P-256, P-384, P-521	Generated internally according to SP 800-133 CKG using SP 800-90A DRBG	Output from the Management Port in plaintext	Plaintext in non-volatile Flash	Factory reset, Filesystem reset	Key agreement within TLS and SSH protocols
SNMP Authentication Password	Passphrase	Manually entered or input from CNFC over TLS in ciphertext	Never output from module	Plaintext in non-volatile Flash	Factory reset, Filesystem reset	Deriving the SNMP Authentication Key
SNMP Encryption Password	Passphrase	Manually entered or input from CNFC over TLS in ciphertext	Never output from module	Plaintext in non-volatile Flash	Factory reset, Filesystem reset	Deriving the SNMP Encryption Key
SNMP Encryption Key	AES-CFB128 key	Derived internally using SNMP KDF	Never output from module	Plaintext in volatile RAM	End SNMP session, Power cycle	Encryption/Decryption for SNMP
SNMP Authentication Key	HMAC SHA-1 key	Derived internally using SNMP KDF	Never output from module	Plaintext in volatile RAM	End SNMP session, Power cycle	Message authentication for SNMP
Firmware Load Test Key	ECDSA P-521 key	N/A	Never output from module	Plaintext in non-volatile Flash	N/A	Digital signature verification
DRBG Entropy Input String	128- to 256-bit value	Generated internally	Never output from module	Plaintext in volatile RAM	End of DRBG function, Power cycle	Random number generation
DRBG Seed	256- to 384-bit value	Gathered internally from NDRNG	Never output from module	Plaintext in volatile RAM	End of DRBG function, Power cycle	Random number generation

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
DRBG Key Value	Internal state value	Generated internally	Never output from module	Plaintext in volatile RAM	End of DRBG function, Power cycle	Random number generation
DRBG 'V' Value	Internal state value	Generated internally	Never output from module	Plaintext in volatile RAM	End of DRBG function, Power cycle	Random number generation

The AES-GCM IV is used in the following protocols:

- TLS – The TLS AES-GCM IV is generated in compliance with TLSv1.2 GCM cipher suites as specified in RFC 5288 and section 3.3.1 of NIST SP 800-52rev1. Per RFC 5246, when the nonce_explicit part of the IV exhausts the maximum number of possible values for a given session key, the module will trigger a handshake to establish a new encryption key.

- IPsec – The IPSec AES-GCM IV is generated in compliance with RFC 5282. When the IV exhausts the maximum number of possible values for a given security association (2^{64} -1), per RFC 7296 a new encryption key will be established. The IPsec Session Key is derived using the KBKDF (rather than IKE). The IPsec KD Message and IPsec Key Derivation Key (used for establishing the IPsec Session Key) are passed in from the calling application over TLS. The protocol has not been reviewed or tested by the CAVP or CMVP.

- SSH – The SSH AES-GCM IV is generated internally at its entirety randomly, using an Approved DRBG whose seed is generated inside the module's physical boundary.

2.8 EMI / EMC

The module was tested and found conformant to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (business use).

2.9 Self-Tests

The module performs power-up self-tests and conditional self-tests. These tests are described in the sections that follow.

Once it has been configured to operate in its Approved mode according to section 3.1.2 below, the module performs power-up self-tests automatically after power is applied; no further intervention is required from the operator. Conditional tests are performed when conditions require. Data output and cryptographic operations are inhibited until the module has successfully passed all the power-up self-tests.

2.9.1 Power-Up Self-Tests

The CEP performs the following self-tests at power-up to verify the integrity of the module firmware and the correct operation of the FIPS-Approved algorithm implementations:

- ECDSA P-521 firmware integrity check
- Known answer tests (KATs)
    - AES-ECB encrypt KAT
    - AES-ECB decrypt KAT
    - AES-GCM encrypt KAT
    - AES-GCM decrypt KAT
    - AES-CMAC encrypt KAT
    - AES-CMAC decrypt KAT
    - HMAC SHA-1 KAT
    - HMAC SHA-256 KAT
    - HMAC SHA-384 KAT
    - HMAC SHA-512 KAT
    - ECDSA pairwise consistency test (PCT)
    - CTR_DRBG KAT
    - ECC CDH primitive ‘Z’ computation KAT

Note: HMAC KATs with SHA-1 and SHA-2 utilize (and thus test) the full functionality of the SHA-1 and SHA-2 algorithms; therefore, no independent KATs for SHA-1 and SHA-2 implementations are required.

2.9.2 Conditional Self-Tests

The CEP performs the following conditional self-tests:

- Continuous RNG test on the NDRNG
- Continuous RNG test on the CTR_DRBG

- ECDSA PCT
- Bypass test
- ECDSA P-521 firmware load test
- SNMP duplicate password entry test

The CEP implements the SP 800-90A CTR_DRBG as its random number generator. The SP 800-90A specification requires that certain health functions be tested conditionally when a random number or asymmetric key is generated to ensure the security of the DRBG. Therefore, the following health tests are implemented by the cryptographic module for the CTR_DRBG:

- DRBG instantiate
- DRBG generate
- DRBG reseed

2.9.3 Critical Functions Self-Tests

There are no critical functions tested by the module.

2.9.4 Self-Test Failure Handling

If any of the self-tests fail (except for the firmware load test and SNMP duplicate password entry test), the module enters a critical error state (e.g. “Failed”), displays an error message on the console, and logs the error. In this state, cryptographic operations are halted, and the module inhibits all data output from the module. The only action available from this state is to power-cycle the module to trigger the re-execution of the power-up self-tests.

To exit the error state, the CO shall power cycle the appliance or use the appropriate command to reboot the appliance via the serial console CLI or CFNC. The error condition is considered to have been cleared if the module successfully passes all of the subsequent power-up self-tests. If the module continues to fail subsequent power-up self-tests, the module is considered to be malfunctioning or compromised, and the module should be sent to Certes for repair or replacement.

If the firmware load test fails, the upgrade process is aborted and no changes are made to the module firmware. If the manual key entry test fails, an error is displayed and the keys must be re-entered.

2.10 Mitigation of Other Attacks

This section is not applicable. The modules do not claim to mitigate any attacks beyond the FIPS 140-2 Level 1 requirements for this validation.

3. Secure Operation

The CEP meets Level 1 requirements for FIPS 140-2. The sections below describe how to place and keep the module in the FIPS-Approved mode of operation.

3.1 Installation and Setup

The CO shall be responsible for receiving, installing, initializing, and maintaining the CEP module. To operate the module in the Approved mode, the CO shall configure the module via the CFNC application or the CLI as mandated by this Security Policy. The following sections provide the CO with important instructions and guidance for the secure installation and configuration of the CEP.

3.1.1 Initial Setup

Upon receiving the CEP hardware, the CO shall check that the system is not damaged and that all required parts and instructions are included. The CO shall refer to the *Certes CryptoFlow Net Creator Installation Guide, Version 5.3 REV A* and the *Certes Enforcers for Certification Product Guide REV A* for initial setup instructions.

After the CO has finished installation of the module, the management interfaces can be accessed to configure the module in the FIPS-Approved mode of operation, which is outlined in section 3.1.2 below.

3.1.2 FIPS-Approved Mode Configuration

The CO shall enable FIPS mode. This ensures that the system will use only FIPS-Approved cryptographic algorithms and key strengths. FIPS mode must be enabled using CFNC. When the module is placed into FIPS mode and powered on, the following actions are automatically performed:

- All applicable power-up self-tests as described in section 2.9.1 are performed during the boot process.
- All conditional tests as described in section 2.9.2 are performed as conditions require.
- All pre-existing policies and keys are cleared. This includes distributed key policies, point-to-point Layer 2 policies, and management port policies. For distributed key policies, traffic is sent in the clear until new encryption policies are created and deployed. For all other policies, keys are automatically renegotiated. Traffic is discarded in the interim.
- All externally signed certificates are removed.
- All passwords are reset to the factory defaults.
- All remote SSH client sessions are terminated.

When disabling FIPS mode, the CO must ensure that all existing CSPs and keys are replaced or deleted.

To configure a CEP, otherwise referred to in the user documentation as Policy Enforcement Point (PEP), for FIPS mode, access the CFNC application, select the PEP to configure, select ‘Edit Multiple PEPs’ and then select ‘Enable FIPS’.

In addition, to prevent access to the USB ports in the FIPS- Approved mode, the CO shall configure each appliance using the following procedure:

1. Attach a terminal to the serial console and enter the BIOS configuration by pressing F2 or DEL immediately after powering on the appliance.
2. Switch to the 'Advanced' tab.
3. Select 'USB Configuration'.
4. Modify the 'USB Support' setting to 'Disabled'.
5. Switch to the 'Security' tab.
6. Select 'Administrator Password' to set a BIOS password to prevent unauthorized changes.
7. Press 'F4' to save changes and reboot the appliance.

3.2 Crypto Officer Guidance

The Crypto Officer is responsible for ensuring that the module is running in its FIPS-Approved mode of operation.

3.2.1 Monitoring Status

The CO shall be responsible for regularly monitoring the module's status to verify that it continues to operate in the FIPS-Approved mode of operation.

- To verify the FIPS mode status of a PEP from the CFNC, from the 'PEP' tab, ensure that the 'FIPS Mode Enabled' box is checked.

  An alternate method exists to select the PEP, right-click on it, and choose 'Diff Config'. Verify that the 'Advanced Setting FIPS Enabled' reports a value of 'true'. If FIPS mode has not been enabled, the setting will report a value of 'false'.

- To verify the FIPS mode status via the CLI, use the 'show fips-status' command and verify the 'Admin Status' is 'fips_on' and 'State' is 'Enabled'. If FIPS mode has not been enabled, the command output will report 'fips_off' and 'Disabled', respectively.

- Bypass capability status is indicated using the 'show spd' command, which will display the policies in effect, their actions, and count of packets matching that policy action. Bypass capability is indicated by the presence of policies with an action of "none".

Power-on self-tests may be executed on-demand by power cycling the module.

3.2.2 Zeroization

All ephemeral keys and CSPs can be zeroized by power-cycling the module. In addition, protocol session (e.g., TLS, SSH, SNMP) keys will automatically be zeroized at the end of the protocol session. Session keys for network encryption will be zeroized automatically after the rekey transition period ends.

Persistently-stored keys and CSPs can be zeroized by restoring the module to factory defaults using the 'filesystem-reset' command. The IPsec KD Message and IPsec Key Derivation Key can also be zeroized using the 'clear-policies' command.

3.2.3 Restoring Factory Defaults

To restore the module to factory defaults, the CO shall use the 'filesystem-reset' command. During this process, the module shall remain in the control of the CO to prevent the compromise of stored CSPs.

3.2.4 Default Operator Passwords

The module provides default passwords for module access. The CO shall ensure that all default passwords are changed immediately after their initial use.

3.3 User Guidance

The User must select strong passwords and must not reveal their password to anyone. Additionally, User role operators must be careful to protect any secret or private keys in their possession.

3.4 Additional Usage Policies

This section notes additional policies (below) that must be followed by module operators:

- The CO shall power-cycle the module if the module has encountered a critical error and becomes non-operational. If power cycling the module does not correct the error condition, the module is considered to be compromised or malfunctioned and should be sent back to Certes for repair or replacement.

- The module allows for the loading of new firmware and employs an Approved message authentication technique to test the new firmware's integrity. However, to maintain an Approved mode of operation, the CO shall ensure that only FIPS-validated firmware is loaded. Any operation of the module after loading non-validated firmware is outside the scope of this Security Policy and will require a separate FIPS 140-2 validation.

- If power to the module is lost and subsequently restored, the CFNC must ensure that any AES-GCM keys used for encryption or decryption are re-distributed.

3.5 Non-Approved Mode

When initialized and configured according to the guidance in section 3.1 of this Security Policy, the module does not support a non-Approved mode of operation.

4. Acronyms

Table 8 provides definitions for the acronyms used in this document.

Table 8 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
BMC	Baseboard Management Controller
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CEP	Certes Enforcement Points
CFB	Cipher Feedback
CFNC	CryptoFlow Net Creator
CKG	Cryptographic Key Generation
CLI	Command Line Interface
CMAC	Cipher-based Message Authentication Code
CMVP	Cryptographic Module Validation Program
CO	Cryptographic Officer
CSE	Communications Security Establishment Canada
CSP	Critical Security Parameter
CTR	Counter
CVL	Component Validation List
DDR	Double Data Rate
DH	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
EC	Elliptic Curve
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
ECC CDH	Elliptic Curve Cryptography Co-factor Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EEPROM	Electrically Erasable Programmable Read-Only Memory
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
GbE	Gigabit Ethernet

Gbps	Gigabits per second
GCM	Galois/Counter Mode
HDD	Hard Disk Drive
HDMI	High-Definition Multimedia Interface
HMAC	(keyed-) Hash Message Authentication Code
HWM	Hardware Monitor
ID	Identifier
IP	Internet Protocol
IPsec	Internet Protocol Security
IV	Initialization Vector
KAT	Known Answer Test
KBKDF	Key-based KDF
KD	Key Derivation
KDF	Key Derivation Function
LAN	Local Area Network
LCD	Liquid Crystal Display
LED	Light Emitting Diode
Mbps	Megabits per second
MPLS	Multiprotocol Label Switching
mSATA	Mini SATA
NDRNG	Non-deterministic RNG
NIST	National Institute of Standards and Technology
PCIe	Peripheral Component Interconnect express
PCH	Platform Controller Hub
PEP	Policy Enforcement Point
PSU	Power Supply Unit
PUB	Publication
RAM	Random Access Memory
RNG	Random Number Generator
SATA	Serial Advanced Technology Attachment
SFP	Small Form-Factor Pluggable
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SNMP	Simple Network Management Protocol
SOC	System On Chip
SP	Special Publication
SSD	Solide State Drive

SSH	Secure Shell
TLS	Transport Layer Security
TPM	Trusted Platform Module
U	Rack Unit
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
XML-RPC	eXtensible Markup Language – Remote Procedure Call

Prepared by:
Corsec Security, Inc.

13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com