

FIPS 140-2 Security Policy
CEP100, CEP100-XSA, CEP1000

Firmware Version 1.4
Hardware Versions: CEP100, A;
CEP100-XSA, A;
CEP1000, A

ECO, Date, and Revision History Rev A Initial release	Contact: Kevin Nigh		CIPHER OPTICS 701 Corporate Center Drive Raleigh, NC 27607	
	Checked:	Approved:		
	Filename: 007-005-001_v7.doc			
	Title: FIPS 140-2 Security Policy CEP100, CEP100-XSA, CEP1000			
Copyright 2009. All rights reserved. This document may be freely copied and distributed without the Author's permission provided that it is copied and distributed in its entirety without modification.	Date: 11/20/2009	Document Number: 007-005-001	Rev: A	Sheet: 1 of 21

Table of Contents

1	Introduction to the CipherOptics CEP Security Policy	3
2	Definition of the CipherOptics CEP Security Policy	4
2.1	CipherOptics CEP Operation Overview	4
2.1.1	CipherOptics CEP Physical Interfaces	4
2.1.2	CEP Logical interfaces	8
2.2	Product Features.....	8
2.3	CipherOptics CEP Technology Overview	10
2.3.1	IP Packet Encryption (Layer 3)	10
2.3.2	Layer 2 Ethernet Frame Encryption.....	11
2.4	Security Rules for FIPS 140-2 Level 2 Operation.....	11
2.4.1	Operational Constraints	11
2.4.2	Security Policy Limitation	11
2.4.3	Discretionary Access Control.....	11
2.4.4	Default Deny	11
2.4.5	Power Requirements	11
2.4.6	Security Modes	12
2.4.7	Physical Level Security	12
2.5	Secure Setup Procedure.....	12
2.5.1	Initiating FIPS Compliant Mode	13
3	Purpose of the CipherOptics CEP Security Policy.....	13
3.1	CipherOptics CEP Security Feature Overview	13
3.2	Module Self-Tests	14
4	Specification of the CipherOptics CEPS Security Policy	15
4.1	Roles	15
4.2	Identification and Authentication Policy	16
4.3	Access Control, Roles, and Services.....	16
4.4	Physical Security Policy	17
4.5	Strength of Function.....	18
5	Crypto Security Officer and User Guidance	18
6	Glossary of Terms	19
7	References	20
8	Revisions.....	20
8.1	Revision History	21

1 Introduction to the CipherOptics CEP Security Policy

This document describes the non-proprietary security policy for the CipherOptics™ CEP100, CEP100-XSA and CEP1000 network security appliances as required and specified in the NIST FIPS-140-2 standard. Under the standard, the CipherOptics CEP appliances qualify as a multi-chip stand-alone cryptographic module and satisfy overall FIPS 140-2 Level 2 security requirements. In this document the CipherOptics CEP models 100, 100-XSA and 1000 are collectively referred to as CEP or Crypto module.

With the exception of this non-proprietary Security Policy, the FIPS 140-2 Validation Documentation is proprietary to CipherOptics Inc, and is releasable only under appropriate non-disclosure agreements.

The CipherOptics CEP encryptors meet the overall requirements applicable for FIPS 140-2 Level 2 Security, as listed in Table 1. This document applies to firmware version 1.4 and the following hardware versions: CEP100 version A, CEP100-XSA version A, and CEP1000 version A.

Table 1: CEP Security Levels

Security Requirements Section	Level
Cryptographic Module Specification	2
Cryptographic Module Ports and Interface	2
Roles and Services and Authentication	3
Finite State Machine Model	2
Physical Security	2
Operational Environments	N/A
Cryptographic key Management	2
EMI/EMC	3
Self-tests	2
Design Assurance	3
Mitigation of Attacks	N/A
Cryptographic Module Security Policy	2

The CipherOptics CEP appliances are in FIPS mode when FIPS mode is enabled on the CEP, the module is powered on and processing traffic. When operating in FIPS mode, only FIPS approved cipher/authentication algorithms are allowed to be used in security policies established by the Crypto Security Officer. FIPs mode is enabled by the Crypto Security Officer.

This security policy is composed of:

A definition of the CipherOptics CEP security policy, which includes:

- an overview of the CipherOptics CEP operation
- a list of security rules (physical or otherwise) imposed by the product developer

A description of the purpose of the CipherOptics CEP security policy, which includes:

- a list of the security capabilities performed by the CipherOptics CEP

Specification of the CipherOptics CEP Security Policy, which includes:

- a description of all roles and cryptographic services provided by the system
- a description of identification and authentication policies

- a specification of the access to security relevant data items provided to a user in each of the roles
- a description of physical security utilized by the system

2 Definition of the CipherOptics CEP Security Policy

2.1 CipherOptics CEP Operation Overview

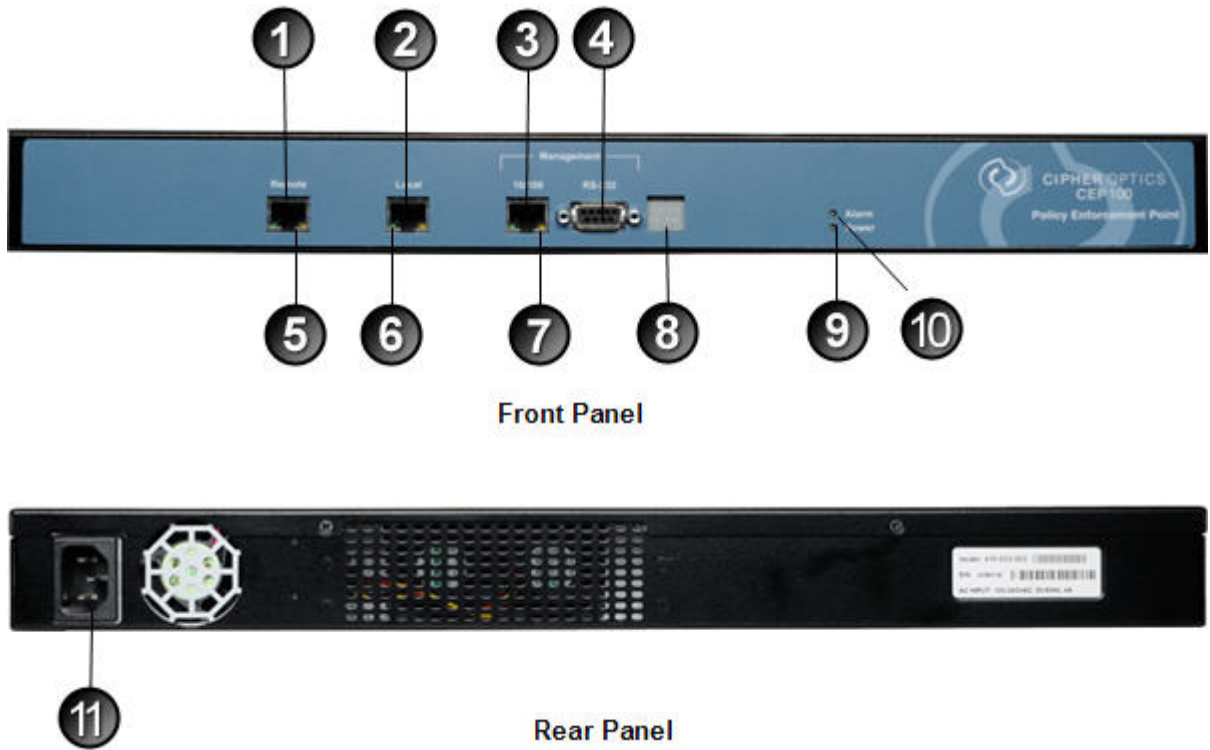
The CipherOptics CEP encryptors are high performance, integrated encryption appliances that offer full line rate IP Packet and Ethernet Frame encryption for 100Mbps and 1Gbps Ethernet transports. Housed in a tamper evident chassis, the CipherOptics CEPs have two functional Ethernet ports used for traffic. The CEP100 and CEP100-XSA have two functional 100 Mbps Ethernet ports and the CEP1000 has two functional Gigabit Ethernet ports. Traffic on the CEP's local port is received from and transmitted to the trusted network in the clear, while traffic on the CEP's remote port has security processing applied to it.

The CEP is capable of encrypting Ethernet Frames (Layer 2) or IP packets (Layer 3). The selection between Ethernet Frame or IP packet encryption is controlled by the CEP configuration and the creation and deployment of a CEP network security policy. From a central location, the Crypto Security Officer defines the network elements to be protected in a CEP Policy. The CEP policy is deployed to the CEP over a secure out-of-band management channel. The module's cryptographic boundary is the module chassis. No components are excluded from the requirements of FIPS PUB 140-2.

2.1.1 CipherOptics CEP Physical Interfaces

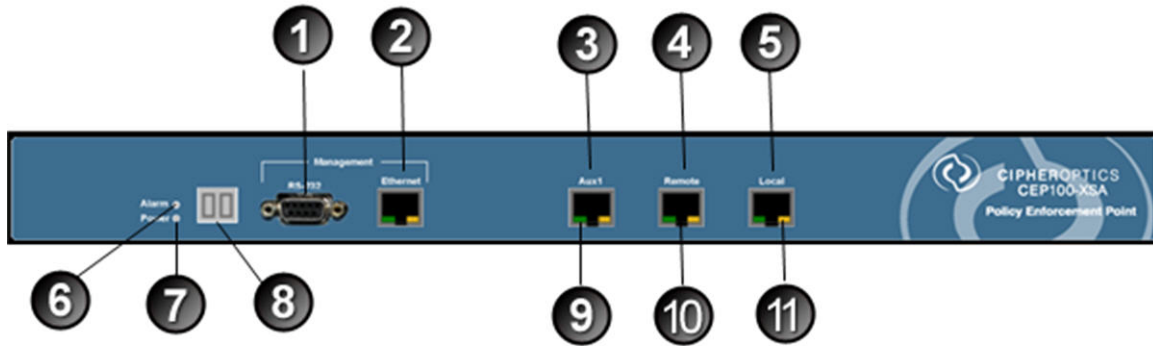
The following figures show the physical layout of the CipherOptics CEP100, CEP100-XSA, and CEP1000. The back of the module contains a standard, enclosed line cord receptacle and cannot be exploited.

Figure 1: CipherOptics CEP100 Physical Layout of Indicators and Receptacles



1. Remote 100 Mbps Ethernet Port
2. Local 100 Mbps Ethernet Port
3. 10/100 Ethernet Management Port
4. RS-232 Management Port
5. Remote Port LEDs
6. Local Port LEDs
7. 10/100 Ethernet Management Port LEDs
8. LCD Boot Status Indicator
9. Power LED
10. Alarm LED
11. Power

Figure 2: CipherOptics CEP100-XSA Physical Layout of Indicators and Receptacles



Front Panel

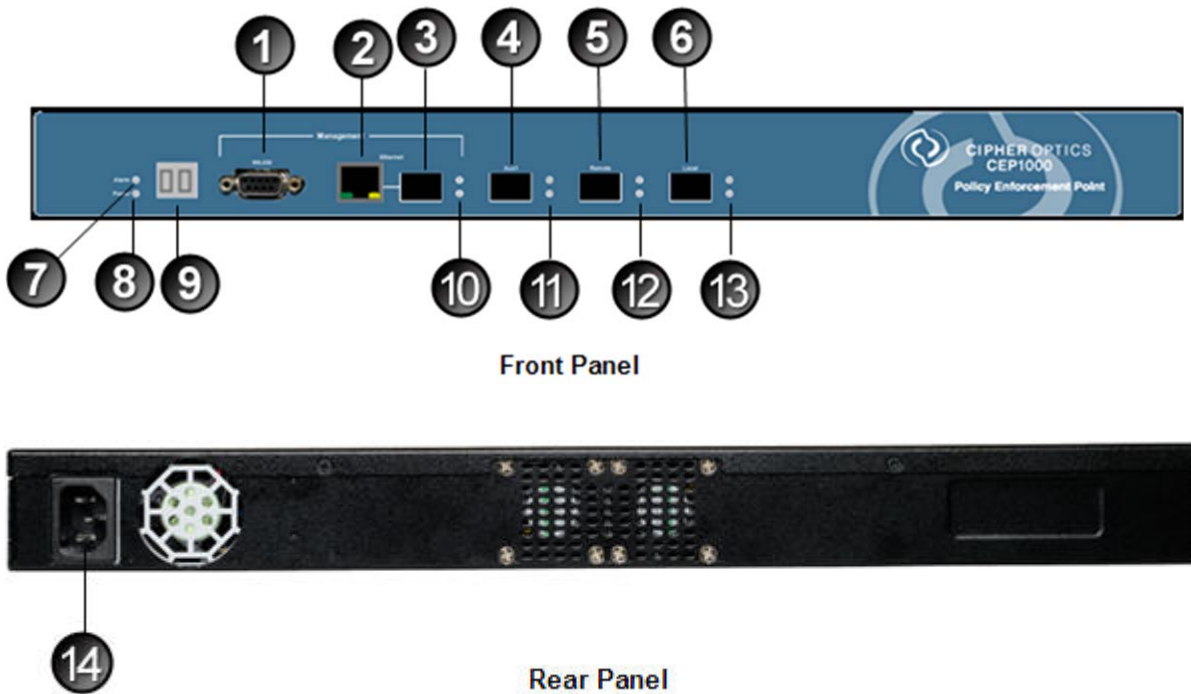


12

Rear Panel

1. RS-232 Management Port
2. 10/100 Ethernet Management Port
3. Aux1 Port (not enabled)
4. Remote 100 Mbps Ethernet Port
5. Local 100 Mbps Ethernet Port
6. Alarm LED
7. Power LED
8. LCD Boot Status Indicator
9. Aux1 Port LEDs
10. Remote Port LEDs
11. Local Port LEDs
12. Power connector

Figure 3: CipherOptics CEP1000 Physical Layout of Indicators and Receptacles



1. RS-232 Management Port
2. 10/100 Ethernet Management Port
3. Gigabit Ethernet Management Port (not enabled)
4. Aux1 Port (not enabled)
5. Remote 1 Gbps Ethernet Port
6. Local 1 Gbps Ethernet Port
7. Alarm LED
8. Power LED
9. LCD Boot Status Indicator
10. Gigabit Management Port LEDs
11. Aux1 Port LEDs
12. Remote Port LEDs
13. Local Port LEDs
14. Power connector

2.1.2 CEP Logical interfaces

Table 2: Mapping of FIPS 140-2 Logical interfaces to the CEP

FIPS 140-2 Logical Interface	CEP100	CEPXSA-100	CEP1000
Data Input	Local Ethernet Port	Local Ethernet Port	Local Gigabit Ethernet Port
Data Output	Remote Ethernet Port	Remote Ethernet Port	Remote Gigabit Ethernet Port
Control Input	Ethernet management port, RS-232 serial port	Ethernet management port, RS-232 serial port	Ethernet management port, RS-232 serial port
Status Output	Ethernet management port, LCD indicator, LED indicators, RS-232 serial port	Ethernet management port, LCD indicator, LED indicators, RS-232 serial port	Ethernet management port, LCD indicator, LED indicators, RS-232 serial port
Power	External power supply	External power supply	External power supply

2.2 Product Features

Hardware-based encryption processing

Low latency

In-line network encryptor

200 Mbps (CEP100 and CEP100-XSA) and 2 Gbps (CEP1000) AES and Triple-DES encryption and decryption

Encrypts Ethernet frames or IP packets

Comprehensive security standards support

Compliant with IPSec RFC 2401, RFC 2406

Layer 3: Encapsulating Security Payload (ESP) supported in Tunnel mode

Layer 2: Security transform using standard AES-256 and SHA-1

Table 3: Approved Security Functions

<i>Approved or Allowed Security Function</i>	<i>CEP100 Certificate</i>	<i>CEP100-XSA, CEP1000 Certificate</i>
<i>Symmetric Key Encryption – Hardware</i>		
AES (CBC, ECB, CFB128, OFB, CTR(int only) (e/d; 128, 192, 256))	465	
AES (CBC, ECB, CFB128, OFB, CTR(int only), CCM (e/d; 128, 192, 256))		762
Triple-DES (TCBC, TECB (e/d; KO 1,2))	482	667
<i>Symmetric Key Encryption – Software</i>		
AES (ECB(e/d; 128,192,256); CBC(e/d; 128,192,256); CFB8(e/d; 128,192,256); CFB128(e/d; 128,192,256); OFB(e/d; 128,192,256))	1210	1210
Triple-DES (TECB(e/d; KO 1,2); TCBC(e/d; KO 1,2); TCFB8(e/d; KO 1,2); TCFB64(e/d; KO 1,2); TOFB(e/d; KO 1,2))	873	873
<i>SHS – Hardware</i>		

SHA-1 and SHA-256 byte-oriented	768	
SHA-1, SHA-256, SHA-384, SHA-512 byte-oriented		769
HMAC-SHA-1 and HMAC-SHA-256	416	
HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512		417
SHS – Software		
SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	1114	1114
HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	705	705
DSA (FIPS186-2: PQG(gen) MOD(1024); KEYGEN(Y) MOD(1024); SIG(gen) MOD(1024); SIG(ver) MOD(1024);	400	400
Asymmetric Keys		
RSA (ANSI X9.31) PKCS #1 V1.5, PSS(Sig Gen and Sig Ver) RSA (ANSI X9.31) Key Generation	582	582
Random Number Generation (ANSI X9.31)	672	672
Non-Approved Security Function		
MD5		
HMAC MD5		
Diffie-Hellman (Key agreement, Key establishment provides 97 bits of encryption strength)		
RSA (Key transport, key establishment provides 80 to 150 bits of encryption strength)		

Encryption

Triple-DES-CBC (168 bit)
AES-CBC (256 bit)

Message integrity

HMAC-MD5-96 (Available in non-FIPS mode only)
HMAC-SHA-1

Signature Generation and Verification

RSA (ANSI X9.31)
Random Number Generation (ANSI X9.31 AES 128)

Device management

Management access via the RS-232 serial port or secure 10/100 Ethernet port
Command line and GUI-based management interfaces
Secure Telnet (SSH) session for limited device configuration and diagnostics
Secure SSL-TLS session for management application, using XML-RPC (see Glossary)
Alarm condition detection and reporting through audit log capability
Secure remote authenticated firmware updates

2.3 CipherOptics CEP Technology Overview

The CipherOptics CEPs can be seamlessly deployed into many network topologies, including IP site-to-site VPNs, MPLS/VPLS networks, storage over IP networks, Metro Ethernet networks and bridged Ethernet wireless networks. The CEP's high-speed AES and Triple-DES processing eliminates bottlenecks while providing data authentication, confidentiality, and integrity.

The AES and Triple-DES algorithms employed by the CipherOptics CEP to encrypt/decrypt all sensitive data, are the current standard for the protection of Unclassified but Sensitive Information for the Federal Government. In addition, the HMAC SHA-1 algorithm is used to provide message integrity and authentication.

A typical operating environment is illustrated in Figure 4.

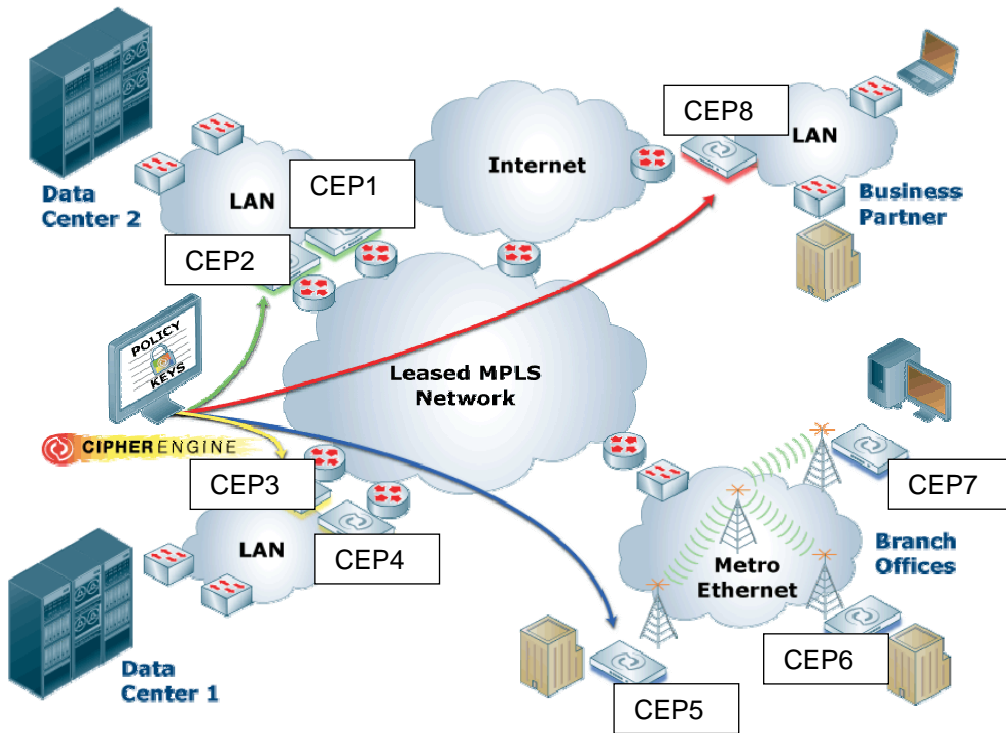


Figure 4: Typical Operational Configuration.

The Crypto Security Officer configures the traffic rules and pushes the resulting policy out to the CEP encryptors. In the illustration above the Metro Ethernet, wireless canopy and MPLS backbones are the untrusted networks. CEPs 1, 2, 3, 4 and 8 are fully meshed, protecting traffic flowing over the MPLS backbone or Internet. CEPs 5, 6, and 7 are securing the Ethernet infrastructure, securing the transmission of data of the wireless canopy or metro Ethernet service.

2.3.1 IP Packet Encryption (Layer 3)

When protecting IP Packets the CEP uses the IPSec suite of security protocols. IPSec is a framework of standards developed by the Internet Engineering Task Force (IETF) that provides a method of securing sensitive information that is transmitted over an unprotected network such as the Internet.

IPSec policies do this by specifying which traffic to protect, how to protect it, and who to send it to. It provides a method for selecting the required security protocols, determining the algorithms to use for the services, and putting in place any cryptographic keys required to provide the requested services. Because the IP layer provides IPSec services, they can be used by any higher layer protocol.

IPSec security services include:

Copyright 2009, CipherOptics Inc. All rights reserved. This document may be freely copied and distributed without the Author's permission provided that it is copied and distributed in its entirety without modification.	Date: 11/20/2009	Document Number: 007-005-001	Rev: A	Sheet: 10 of 21
--	----------------------------	--	------------------	---------------------------

- Data confidentiality - The sender can encrypt packets before sending them across a network, providing assurance that unauthorized parties cannot view the contents.
- Data integrity - The receiver can authenticate packets sent by the IPSec sender to ensure that the data has not been altered in transit.
- Data origin authentication -The receiver can authenticate the identity of the sender. This service is dependent on the data integrity service.

2.3.2 Layer 2 Ethernet Frame Encryption

At Layer 2, the CEP supports two types of encryption policies: distributed key policies for mesh networks and IKE policies for point-to-point encryption. In Layer 2 distributed key policies the CEP provides encryption services to Ethernet frames by using a VLAN ID as an encryption selector or by encrypting all Ethernet frames received from the trusted network. IKE policies encrypt all Ethernet frames received from the trusted network. The CEP uses hard-coded encryption and authentication algorithms (AES, SHA-1). Because the CEP is encrypting and authenticating the Ethernet frame, any Layer 3 data payload can be encrypted for confidential transmission.

CEP Layer 2 security services include:

- Data confidentiality - The sender can encrypt packets before sending them across a network, providing assurance that unauthorized parties cannot view the contents.
- Data integrity - The receiver can authenticate packets sent by the sender to ensure that the data has not been altered in transit.
- Data origin authentication -The receiver can authenticate the identity of the sender. This service is dependent on the data integrity service.

2.4 Security Rules for FIPS 140-2 Level 2 Operation

The CipherOptics CEP is bound by the following rules of operation to meet FIPS 140-2 Level 2 requirements.

2.4.1 Operational Constraints

The CipherOptics CEP appliance encryption module shall be operated in accordance with all sections of this security policy. The module shall be operated in accordance with all accompanying user documentation.

- CipherOptics CEP Installation & Maintenance Guide
- CipherEngine User Guide

2.4.2 Security Policy Limitation

This security policy is constrained to the hardware and firmware contained within the cryptographic security boundary.

2.4.3 Discretionary Access Control

Discretionary access control based roles shall be assigned in accordance with this security policy.

2.4.4 Default Deny

This module is shipped with all encryption mechanisms disabled to allow installation test and acceptance. Prior to operation, encryption mechanisms shall be enabled, and the module placed in a default deny operational mode.

2.4.5 Power Requirements

It is assumed that this module is being powered at the specified line voltage and that the internal DC power supply is operating normally.

2.4.6 Security Modes

When operating in FIPS mode, the CipherOptics CEP must always use FIPS approved encryption and message authentication in security policies: AES, Triple DES, and SHA-1.

The CipherOptics CEP Ethernet management interface must always operate using FIPS-approved cipher/authentication algorithms – AES or Triple-DES, and SHA-1 authentication. TLS is used for configuration and policy management. SSH is used to secure the command line interface session.

2.4.7 Physical Level Security

The CipherOptics CEP appliance shall be installed in a controlled area with authorized personnel access only. The module also provides security in the form of a tamper evident seal, as shown in Figure 5.

Figure 5. Tamper evident seal is located on the left side panel



2.5 Secure Setup Procedure

The CipherOptics CEP appliance must be set up, installed, and operated in accordance with the instructions in the CEP Installation & Maintenance Guide and the CipherEngine User Guide.

The CipherOptics CEP is shipped with all encryption mechanisms disabled to allow installation test and acceptance. Prior to operation, encryption mechanisms should be enabled.

The CipherOptics appliance's tamper-evident seal must be intact. If the tamper-evident seal is broken, the CipherOptics CEP is not FIPS-140-2 Level 2 compliant.

The following software must be installed on the management workstation:

- CipherOptics CipherEngine software (XML-RPC interface)
- VT-100 terminal emulation utility such as HyperTerminal or TeraTerm Pro (used to connect to the CLI through a serial link)
- Adobe Acrobat Reader version 6.0 or higher, used to open the PDFs files on the product CD)

The following operating systems are supported:

- Microsoft Windows XP with Service Pack 2
- Microsoft Windows 2003 Server

2.5.1 Initiating FIPS Compliant Mode

As stated in Section 2.5, the CipherOptics CEP appliance is shipped with all encryption mechanisms disabled. You must do the following to operate the appliance in a FIPS-compliant mode.

1. Log in to the CLI as the Crypto Security Officer or Operator and set the management port IP address, network mask and network gateway for the module.
2. As the Crypto Security Officer, use the XML/RPC interface to change the default CEP passwords for both the Crypto-Security Officer and Operator roles. CEP passwords must be a minimum of 6 characters, and composed of upper and lowercase characters, numeric characters, and special characters (!@#\$\$%^&*{[]}<>?).
3. As the Crypto Security Officer, enable FIPS mode.
4. As the Crypto Security Officer, create and load a new security policy to encrypt data.
5. Verify that FIPS mode is set to true.

3 Purpose of the CipherOptics CEP Security Policy

CipherOptics CEP encryptors are high performance, integrated encryption appliances that offer full line rate IP Packet and Ethernet Frame encryption for 100Mbps and 1Gbps Ethernet transports. Housed in a tamper evident chassis, the CipherOptics CEPs have two functional Ethernet ports used for traffic. The CEP100 and CEP100-XSA have two functional 100 Mbps Ethernet ports, and the CEP1000 has two functional Gigabit Ethernet ports. Traffic on the CEP's local port is received from and transmitted to the trusted network in the clear, while traffic on the CEP's remote port has security processing applied to it.

The AES and Triple DES algorithms employed by the CipherOptics CEPs to encrypt/decrypt all sensitive data are the current standard for the protection of Unclassified but Sensitive Information for the Federal Government. In addition, the HMAC SHA-1 algorithm is used to provide message integrity and authentication

3.1 CipherOptics CEP Security Feature Overview

Security Features

Hardware-based IPsec encryption processing
Comprehensive security standards support
Compliant with RFC 2401, RFC 2406
Layer 3: Encapsulating Security Payload (ESP) supported in Tunnel mode
Layer 2: Security transform using standard AES-256 and SHA-1

Key Management

Internet Key Exchange (IKE) and ISAKMP, RFCs 2408, 2409

Key Exchange / Key Establishment

Authenticated Diffie-Hellman key exchange (1536 bit modulus)
RSA (Key transport)

Key Types

Table 4: Key Types

Key Name	Description and /or Purpose	Type of Key	Storage Location	Storage Method
Session Encryption Key	One Symmetric Key per IPsec Security Association (SA) or DistKey (SA)	32 Byte AES, 24 Byte Triple-DES (Distkey only)	Non-volatile Flash	Plain-text
Session Authentication Key	One Authentication Key per IPsec Security Association (SA) or DistKey (SA)	20 Byte HMAC-SHA-1	Non-volatile Flash	Plain-text
Management	Encrypt messages to and from	256 Bit AES	Non-volatile Flash	Plain-text

Key Name	Description and /or Purpose	Type of Key	Storage Location	Storage Method
Session Key	the management tool	168 Bit Triple DES		
CipherOptics CEP Identification Keys	Authenticate messages to and from the management tool	1024 Bit RSA Public/Private	Non-volatile Flash	Plain-text
Firmware Upgrade Key	Authenticates firmware to be loaded.	1024 Bit RSA Public	Non-volatile Flash	Plain-text
RNG Key	Used with the ANSI X9.31 RNG	AES	Volatile RAM	Plain-text

Encryption

Triple-DES-CBC (168 bit)
AES-CBC (256 bit)

Hashing

SHA-1
SHA-224
SHA-256
SHA-384
SHA-512
MD5 (Non-FIPS mode)

Message integrity

HMAC-MD5-96 (Available in non-FIPS mode only)
HMAC-SHA-1

Signature Generation and Verification

RSA (ANSI X9.31, PKCS 1.5, PSS)

Random Number Generation

ANSI X9.31

Device management

Management access via the RS-232 serial port or secure 10/100 Ethernet port
Command line and GUI-based management interfaces
Secure Telnet (SSH) session for limited device configuration and diagnostics
Secure SSL-TLS session for management application, using XML-RPC (see Glossary)
Alarm condition detection and reporting through audit log capability
Secure remote authenticated firmware updates

Zeroization

Sets module to factory default keys
Sets module to factory default policies
Sets module to factory default configurations
All plaintext keys are zeroized

Role and Identity Based Access Control

Access to security configuration and device management is controlled by strict userid/password authentication.

3.2 Module Self-Tests

As required by FIPS 140-2, the module performs the following self-tests at start-up:

Power-Up Tests:

AES Known Answer Test
Triple-DES Known Answer Test
HMAC-SHA-1 Known Answer Test
HMAC SHA-224 Known Answer Test
HMAC SHA-256 Known Answer Test

HMAC SHA-384 Known Answer Test
 HMAC SHA-512 Known Answer Test
 SHA-1 Known Answer Test
 RSA Known Answer Test
 RNG Known Answer Test
 Firmware Integrity Test (RSA signature verification 1024 bit public key)
 DSA pairwise consistency test

Continuous Random Number Generator Test:

The CipherOptics CEP includes a continuous test on the output from the FIPS compliant RNG to ANSI X9.31. The module compares the output of the RNG with the previous output to ensure the RNG has not failed to a constant value.

Conditional Pairwise Consistency Test:

The CipherOptics CEP includes a conditional pairwise consistency test (sign and verify operation) every time RSA and DSA keys are generated.

Conditional Bypass Test:

The CipherOptics CEP includes a conditional bypass test that is performed every 15 seconds. The test is a 1024 bit RSA signature verification.

Firmware Load Test:

The CipherOptics CEP includes a firmware load test with an RSA signature verification of downloaded firmware. In order for the module to maintain FIPS compliance the firmware to be upgraded must be validated to FIPS 140-2.

If any of these self-tests fail when the CEP is in FIPS mode, the module is zeroized. During zeroization, the module enters an error state and all data is inhibited. Running of the power-on self-tests is automatically initiated whenever power to the module is cycled or, on demand, by issuing the “reboot” command. During self-tests, the data ports are inhibited until all power-on self-tests pass.

4 Specification of the CipherOptics CEPS Security Policy

4.1 Roles

Three roles, which either provide security services or receive services of the CipherOptics CEP, are the basis of the specification of the CipherOptics CEP security policy. These roles are:

Operator (OPS): The Operator role consists of the Ops user. The role is limited to configuring the management port IP address, viewing the output of show commands (status information), and shutting down and rebooting the CEP.

Crypto Security Officer (CSO): The Crypto Security Officer role consists of the Admin user. The role controls access to the CipherOptics CEP by maintaining all identity-based userid/password configurations. The role views the audit logs on the CEP. The role defines and implements all security and network services. The role specifies the traffic to have security algorithms applied and the transforms to be applied, defines the Ethernet network interfaces and remote management mechanisms, and performs any firmware updates or network troubleshooting.

Network User (User): The User role uses the security services implemented on the CipherOptics CEP. The Network User is any CipherOptics CEP that is authenticated with another CipherOptics CEP to perform encryption and decryption services. The CipherOptics CEP receives user traffic on its local port. It then applies the security services to that traffic and transmits the traffic out the remote port. In addition, the CipherOptics CEP can receive encrypted traffic on its remote port, decrypt the traffic and transmit the traffic to the user on the local port.

4.2 Identification and Authentication Policy

Login by UserID and Password, which are maintained by the Crypto Security Officer, is the primary Identification/Authentication mechanism used to enforce access restrictions for performing or viewing security relevant events. Each operator uses a unique password.

Table 5: Identification/Authentication Policy

Role	Identification/ Authentication	Strength of Authentication
Operator (OPS)	Ops UserId/Password	1: $3.3 * 10^{-62}$
Crypto Security Officer (CSO)	Admin UserId/Password	1: $3.3 * 10^{-62}$
Network User (User)	Session authentication key/20 byte HMAC-SHA-1	1: 10^{24}

Note: Any reference to CSO, Admin, Ops and User in the Access Control, Roles, and Services section indicates the Identification/Authentication as found in Table 5.

4.3 Access Control, Roles, and Services

Table 6 defines the services, the roles that use the services, the security relevant objects created or used in the performance of the service, and the form of access given to those security relevant objects.

The cryptographic boundary for the implementation of these services extends to the physical dimensions of a CipherOptics CEP module and includes all internal printed circuit cards, integrated circuitry, and so forth contained within its physical dimensions.

Note: Items highlighted in yellow are Services with the description of Services detailed directly below the highlighted area.

Table 6: Roles and Services

Roles	CEP Services	Security Relevant Data Item	SRDI Access Read, Write, Execute
CSO	Create Users		
	Create, change, or delete Ops and Admin users	None	Write, Execute
CSO	Change Passwords		
	Change the Ops and Admin passwords.	Password	Write, Execute
CSO	Set Audit Log		
	Sets the audit-log parameters such as log level and where the logs will be sent.	None	Write
CSO	View Audit Log		
	Views the audit-log information.	None	Read
CSO	Zeroization		
	Zeroize the CipherOptics CEP.	Triple DES, AES, CEP Identification keys, Passwords, RNG key	Execute
CSO OPS	Run Self-Test		
	Self-test (critical function test, memory test, encrypt hardware test, algorithm self-tests, firmware authentication, RNG test).	None	Execute
CSO	Key Generation		
	Generate symmetric and asymmetric keys.	Triple DES, AES, RSA	Write, Execute
CSO OPS	Configure		
	CSO: Configure IP addresses, subnets, logging, port settings, policy type (IKE or Distkey), FIPS mode.	None	Read, Write, Execute

Roles	CEP Services	Security Relevant Data Item	SRDI Access Read, Write, Execute
	OPS: Configure management port IP address, mask, and gateway.		
CSO	Enable FIPS Mode		
	Sets the CEP in a FIPS-compliant mode of operation, and runs FIPS self-tests and integrity tests.	None	Write, execute
CSO	Create Security Policy		
	Configure Security Policy Filters, Encryption algorithms, Hash algorithms, set expiration of key lifetime.	Triple DES, AES, RSA	Read, Write, Execute
CSO OPS	Show Status		
	OPS: Display appliance configuration, version information, FIPs mode, NTP status, and log data (system, dataplane, distkey, pki, and snmp-traps). CSO: Display everything from OPS, plus audit log, MAC statistics, encryption statistics, discards, port status, security policy information (SAD and SPD).	None	Read
CSO OPS	Reboot		
	Reboot the CipherOptics CEP.	None	Execute
CSO	Edit Security Policy		
	Update the security policy rules of the CipherOptics CEP.	Triple DES, AES, RSA	Read, Write
CSO	Load Security Policy		
	Load an updated or saved security policy into the CipherOptics CEP.	None	Execute
CSO	Firmware Upgrade		
	Update the firmware of the CipherOptics CEP.	RSA	Execute
CSO	Key Establishment		
	Create a secure session using public/private keys.	RSA, Diffie-Hellman, AES, Triple DES	Execute
CSO	Restore-Filesystem		
	Restores the backup copy of the crypto module filesystem	None	Execute
CSO OPS	Shutdown		
	Orderly Crypto Module shutdown	None	Execute
User	Encrypt/Decrypt		
	Encrypt/Decrypt network traffic.	AES/Triple DES session key, IPSec Session Authentication Key	Execute

4.4 Physical Security Policy

The CipherOptics CEP has been designed by CipherOptics to satisfy the Level 2 physical security requirements of FIPS 140-2. The appliance is housed in an opaque, aluminum chassis with external connections provided for the local and remote data network ports, Auxiliary network port (not enabled), as well as the RS-232 serial port, 10/100 Ethernet management port, and status LEDs. The top lid and baseboard sub-assembly are attached to the case using screws. A tamper evident seal is provided over one screw in such a manner that an attempt to remove the cover requires removal of that screw and indicates subsequent evidence of tampering (see Figure 6).

The Crypto Security Officer shall periodically check the tamper evident seal to verify that the module has not been opened. If the seal is broken, the security policies and tamper seal must be replaced.

Figure 6. Tamper evident seal, located on the left side panel



4.5 Strength of Function

Within the cryptographic security boundary, the CipherOptics CEP appliance will act only on traffic for which a security policy has been defined. Therefore any data received for which no policy exists will be discarded. In addition, any clear traffic destined for the CipherOptics CEP's network address will be discarded. The appliance does not contain a bypass service. The appliance encrypts all upper layer protocol information, thus port scans and DOS attacks are mitigated.

A secure environment relies on security mechanisms, such as firewalls, intrusion detection systems and so forth, to provide mitigation of other attacks, which could lead to a loss of integrity, availability, confidentiality, or accountability, outside of the cryptographic security boundary. Further, no mitigation is provided against clandestine electromagnetic interception and reconstruction or loss of confidentiality via covert channels (such as power supply modulation), or other techniques, not tested as part of this certification.

5 Crypto Security Officer and User Guidance

Service	Access Interface		Role Permissions		
	CLI	XML/RPC	CSO	OPS	User
Create Users		✓	✓		
Change Passwords		✓	✓		
Set Audit Log		✓	✓		
View Audit Log	✓	✓	✓		
Zeroization	✓		✓		
Run Self-Test	✓	✓	✓	✓	
Key Generation		✓	✓		
Configure	✓	✓	✓	✓	
Create Security Policy		✓	✓		
Show Status	✓	✓	✓	✓	

Service	Access Interface		Role Permissions		
	CLI	XML/RPC	CSO	OPS	User
Reboot	✓	✓	✓	✓	
Edit Security Policy		✓	✓		
Load Security Policy		✓	✓		
Firmware Upgrade	✓	✓	✓		
Key Establishment		✓	✓		
Restore-File system	✓	✓	✓		
Shutdown	✓	✓	✓	✓	
Enable FIPS Mode	✓	✓	✓		
Encrypt/Decrypt					✓

6 Glossary of Terms

AES

Advanced Encryption Standard

Authentication

Authentication is the process of identification of a user, device or other entity, (typically based on a password or pass phrase) known only to a single user, which when paired with the user's identification allows access to a secure resource.

Confidentiality

Confidentiality is the assurance that information is not disclosed to unauthorized persons, processes, or devices.

CSP

Critical Security Parameter

Crypto Security Officer (ADMIN)

The Crypto Security Officer is the individual responsible for controlling access to the CipherOptics CEP appliance by maintaining all role-base userid/password configurations. The CSO is also responsible for all security protections resulting from the use of technically sound cryptographic systems. The Crypto Security Officer duties are defined within this document.

Network User (User)

The Network User is a CipherOptics CEP device that has authenticated with a remote CipherOptics CEP device to perform encryption/decryption services between one or more CipherOptics CEPs.

End to End Encryption

The totality of protection of information passed in a telecommunications system by cryptographic means, from point of origin to point of destination.

IKE

Internet Key Exchange

IP

Internet Protocol

IPSEC

Security standard for IP networks

NIST

National Institute of Standards and Technology

Operator (Ops)

The Operator is the individual responsible for initial setup of the management IP address and can monitor status. The Operator duties are defined within this document.

Role

A Role is a pre-defined mission carrying with it a specific set of privileges and access based on required need-to-know basis.

Session Key

An encryption or decryption key used to encrypt/decrypt the payload of a designated packet.

Security Policy

The set of rules, regulations and laws which must be followed to ensure that the security mechanisms associated with the CipherOptics CEP are operated in a safe and effective manner. The CipherOptics CEP Security Policy shall be applied to all Ethernet or IP data flows through the CipherOptics CEP per FIPS 140-2 (Level 2) requirements. It is an aggregate of public law, directives, regulations, rules, and regulates how an organization shall manage, protect, and distribute information.

Tunnel

Logical IP connection in which all data packets are encrypted.

XML-RPC

A Remote Procedure Calling protocol having a set of implementations that allow software running on disparate operating systems, running in different environments to make procedure calls over the Internet. Its remote procedure calling uses TLS as the transport and XML as the encoding. XML-RPC is designed to be as simple as possible, while allowing complex data structures to be transmitted, processed and returned.

Triple DES

Triple DES (Data Encryption Standard)

7 References

Federal Information Processing Standard Publication 140-2 "Security Requirements for Cryptographic Modules"

CipherOptics CEP Installation & Maintenance Guide, Part Number 800-032-001, Rev E, October 2009

CipherEngine User Guide, Version 1.7, Part Number 800-300-001, Rev C, October 2009

CipherOptics CEP FIPS 140-2 Vendor Evidence Document, June 11, 2009

Finite State Machine Document, June 11, 2009

8 Revisions

This document is an element of the Federal Information Processing Standard (FIPS) Validation process as defined in Publication 140-2. Additions, deletions, or other modifications to this document are subject to document configuration management and control. No changes shall be made once stamped FINAL, without the express approval of the Document Control Officer (DCO).

8.1 Revision History

Revision	Change Description	Change Document	Approved
A	Original Issue		