FIPS 140-2 Security Policy

CEP100, CEP100 VSE, CEP100-XSA, CEP1000, CEP1000-DP, CEP1000 VSE

Firmware Version 2.1

Hardware Versions:

[CEP100, A], [CEP100 VSE, A], [CEP100-XSA, A], [CEP1000, A], [CEP1000-DP, A] and [CEP1000 VSE, A]

ECO, Date, and Revision History
Rev A Initial release 9/14/2010
Rev B Updated for CEP 1.6 and VSE
Rev C Updated for CEP2.1
Rev D Update
Rev E Minor Updates 6/14/2012
Rev F Minor Updates 7/18/2012
Rev G Minor Updates 8/28/12

Contact: Todd Cignetti
Checked: Approved:
Filename: CEP10_2-1FIPS_SecurityPolicy.doc

Certes Networks
300 Corporate Center Dr.
Moon Township, PA 15108

Title: **FIPS 140-2 Security Policy : CEP100, CEP100 VSE, CEP100-XSA, CEP1000, CEP1000 VSE**

Table of Contents

1 Introduction to the Certes Networks CEP Security Policy

This document describes the non-proprietary security policy for the CEP100, CEP100 VSE, CEP100-XSA, CEP1000, CEP1000-DP and CEP1000 VSE network security appliances as required and specified in the NIST FIPS-140-2 standard. Under the standard, the CEP appliances qualify as a multi-chip stand-alone cryptographic module and satisfy overall FIPS 140-2 Level 2 security requirements. The cryptographic boundary for the CEP is defined as the entire device with the exception of the CEP1000-DP and CEP 1000 VSE where the dual power supplies have been excluded from the requirements of FIPS PUB 140-2 as they do not process any keys or critical security parameters. In this document the CEP models 100, 100 VSE, 100-XSA, 1000, 1000-DP and 1000 VSE 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 Certes Networks Inc, and is releasable only under appropriate non-disclosure agreements.

The 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 2.1 and the following hardware versions: [CEP100, A], [CEP100 VSE, A], [CEP100-XSA, A], [CEP1000, A], [CEP1000-DP, A] and [CEP1000 VSE, A].

Table 1: CEP Security Levels

Security Requirements Section	Level
Cryptographic Module Specification	3
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 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 CEP security policy, which includes:

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

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

- a list of the security capabilities performed by the CEP

Specification of the 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 Certes Networks CEP Security Policy

2.1 CEP Operation Overview

The CEP encryptors are high performance, integrated encryption appliances that offer full line rate IP Packet and Ethernet Frame encryption for Ethernet transports at variable or fixed rates. The CEP100 VSE offers variable rates of 100Mbps, 155Mbps and 250Mbps. The CEP100-XSA, CEP1000 and CEP1000 VSE offer 1Gpbs rates. Housed in a tamper evident chassis, the CEPs have two functional Ethernet ports used for traffic. 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.

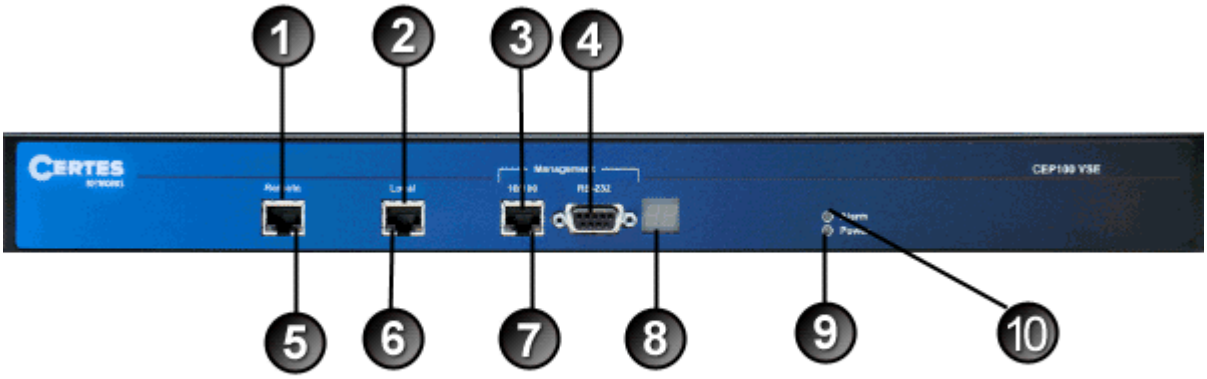
The CEP is capable of encrypting Ethernet Frames (Layer 2) or IP packets (Layer 3). The selection between Ethernet Frame or IP packet encryption is controlled by the CEP configuration and the creation and deployment of a CEP network security policy. From a central location, the Crypto Security Officer 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. Simple policies can also be configured via the Command Line Interface (CLI). The module's cryptographic boundary is the module chassis. No components are excluded from the requirements of FIPS PUB 140-2 except for the dual power supplies present in the CEP1000-DP and CEP1000 VSE models.

A bypass security policy can be set in the security policy file to allow certain data to be transmitted without encryption. There are two steps required in order to enable a bypass function. First, the security policy must be updated to add an entry for the bypass function. Second, the contents of the security policy must be hashed. The CEP will not implement a security policy without verifying the file against its associated hash. If the verification fails, the CEP will enter the error state.

2.1.1 CEP Physical Interfaces

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

Figure 1: CEP100 and CEP100 VSE Physical Layout of Indicators and Receptacles

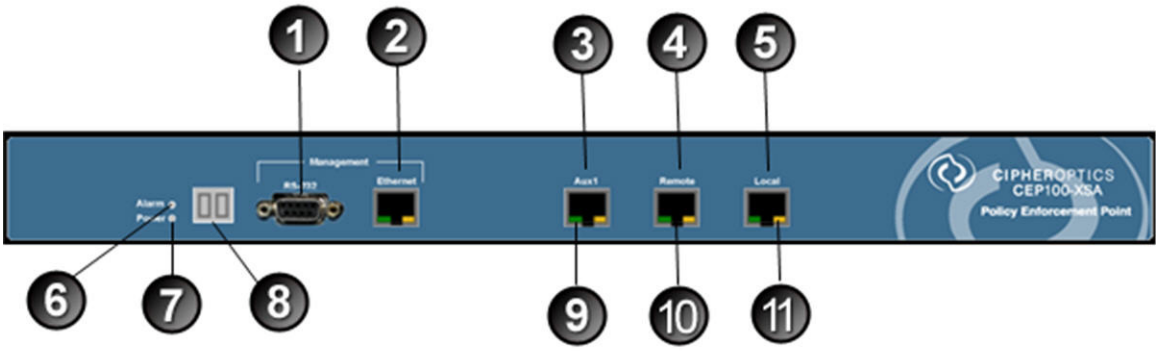


Front Panel

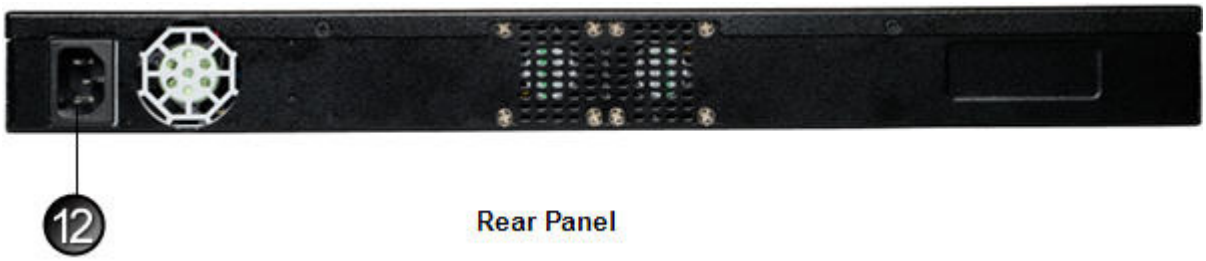
Rear Panel

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

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



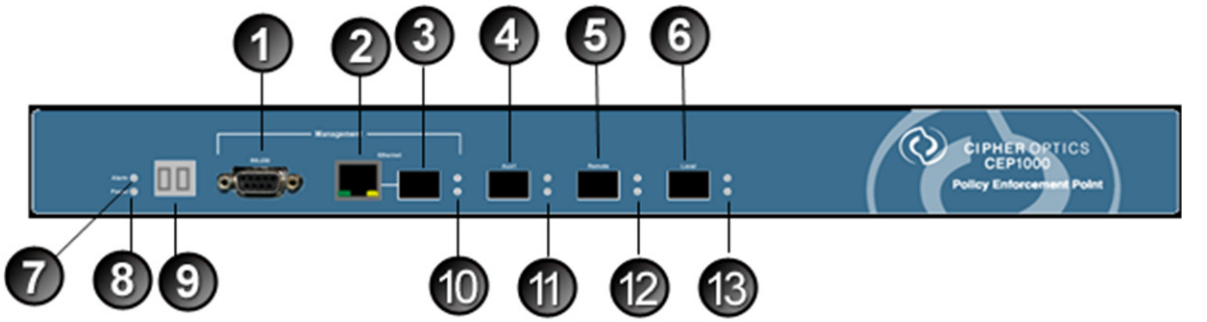
Front Panel



Rear Panel

1. RS-232 Management Port
2. Ethernet Management Port
3. Aux1 Port (not enabled)
4. Remote 1Gbps Ethernet Port
5. Local 1Gbps 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: CEP1000 Physical Layout of Indicators and Receptacles

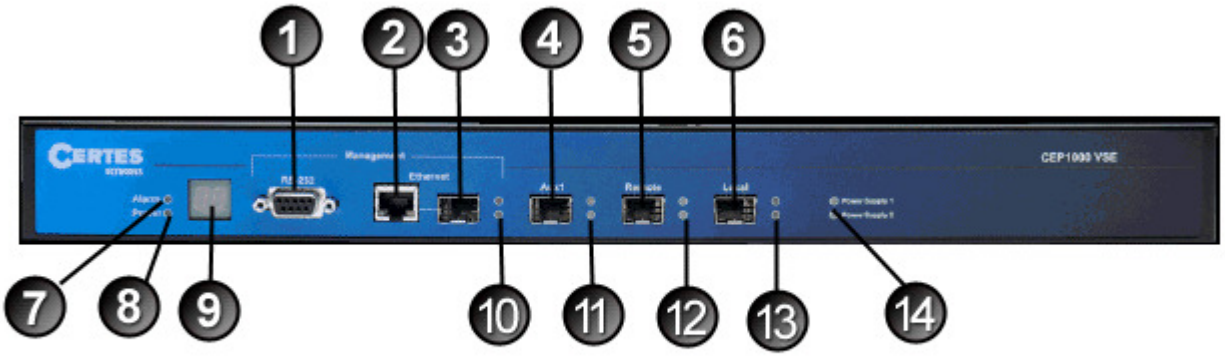


Front Panel

Rear Panel

1. RS-232 Management Port
2. 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

Figure 4: CEP1000-DP and CEP1000 VSE Physical Layout of Indicators and Receptacles



Front Panel

-

Rear Panel

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. Dual Power Supply LEDs
15. Power Connector for Power Supply 2
16. Power Connector for Power Supply 1

2.1.2 CEP Logical interfaces

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

FIPS 140-2 Logical Interface	CEP100, CEP100 VSE	CEPXSA-100	CEP1000	CEP1000-DP CEP1000 VSE
Data Input	Local RJ45 Ethernet Port	Local RJ45 Ethernet Port	Local SFP Transceiver Ethernet Port	Local SFP Transceiver Ethernet Port
Data Output	Remote RJ45 Ethernet Port	Remote RJ45 Ethernet Port	Remote SFP Transceiver Ethernet Port	Remote SFP Transceiver 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	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	Ethernet management port, LCD indicator, LED indicators, RS-232 serial port
Power	Integrated PS	Integrated PS	Integrated PS	Dual Redundant PS

2.2 Product Features

Hardware-based encryption processing
Low latency
In-line network encryptor
200 Mbps, 310Mbps, 500Mbps (CEP100, CEP100 VSE) and 2 Gbps (CEP100-XSA, CEP1000, CEP1000-DP, CEP1000 VSE) 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 HMAC-SHA-1

Table 3: Approved Security Functions in Hardware

Approved or Allowed Security Function	***CEP100, CEP100 VSE Certificate***	***CEP100-XSA, CEP1000, CEP1000-DP, CEP1000 VSE Certificate***
Symmetric Encryption – Hardware		
AES CBC (e/d: 256)	465	762
Triple-DES (TCBC)	482	667
HMAC – Hardware		
HMAC-SHA-1 and HMAC-SHA-256	416	417
Non-Approved Security Function		
MD5		
HMAC-MD5-96		

Table 4: Approved Security Functions in Certes Networks CEP Cryptographic Library

Approved or Allowed Security Function	*CEP100, CEP100 VSE Certificate*	*CEP100-XSA, CEP1000, CEP1000-DP, CEP1000 VSE Certificate*
Symmetric Encryption – Firmware		
AES (ECB(e/d; 128,192,256); CBC(e/d; 128,192,256); CFB8(e/d; 128,192,256); OFB(e/d; 128,192,256); OFB128(e/d; 128,192,256))	1932	1932
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))	1258	1258
SHS – Firmware		
SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	1697	1697
HMAC – Firmware		
HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	1166	1166
Digital Signatures – Firmware		
DSA (FIPS186-2: PQG(gen) MOD(1024); PQG(ver) MOD(1024); KEYGEN(Y) MOD(1024); SIG(gen) MOD(1024); SIG(ver) MOD(1024)	615	615
RSA [ANSIX9.31]; Key(gen)(MOD: 1024 , 1536 , 2048 , 3072 , 4096 PubKey Values: 3 , 17 , 65537) **[ANSIX9.31]; SIG(gen); SIG(ver); 1024 , 1536 , 2048 , 3072 , 4096 , SHS: SHA-1, SHA-256, SHA-384, SHA-512** **[RSASSA-PKCS1_V1_5]; SIG(gen); SIG(ver); 1024 , 1536 , 2048 , 3072 , 4096 , SHS: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512** **[RSASSA-PSS]; SIG(gen); SIG(ver); 1024 , 1536 , 2048 , 3072 , 4096 , SHS: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512**	998	998
Random Number Generation		
ANSI X9.31 **[AES-128Key AES-192Key AES-256Key]**	1017	1017
Non-Approved Security Function		
MD5		
HMAC MD5		
Diffie-Hellman (Key agreement, Key establishment provides 80 to 150 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)
AES-CBC (192 bit)
AES-CBC (128 bit)

Message integrity
HMAC-MD5-96 (Available in non-FIPS mode only)
HMAC-SHA-1
HMAC-SHA-256
HMAC-SHA-384
HMAC-SHA-512

Signature Generation and Verification
RSA, DSA

Random Number Generation
ANSI X9.31

Device Management
Management access via the RS-232 serial port or secure 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 (via SFTP and SCP)
SNMPv2 (Available in non-FIPS mode only)
SNMPv3 – Non-security related monitoring and queries only can be done via SNMP. Only SNMPv3 with security level noAuthNoPriv or authNoPriv using HMAC-SHA-1 is permitted by this security policy. If authNoPriv security level is used, the user passwords shall be at least 8 or more characters including numbers and letters. SNMPv3 using encryption (authPriv) is not permitted in FIPS mode.

2.3 CEP Technology Overview

The CEPs can be seamlessly deployed into many network topologies, including IP site-to-site VPNs, MPLS/VPLS networks, public internet service, 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 CEP employs AES and Triple-DES algorithms to encrypt/decrypt all sensitive data. These are the current standard for the protection of Unclassified but Sensitive Information for the Federal Government. In addition, the HMAC SHA-1 and SHA-2 algorithms are used to provide message integrity and authentication.

A typical operating environment is illustrated in Figure 5.

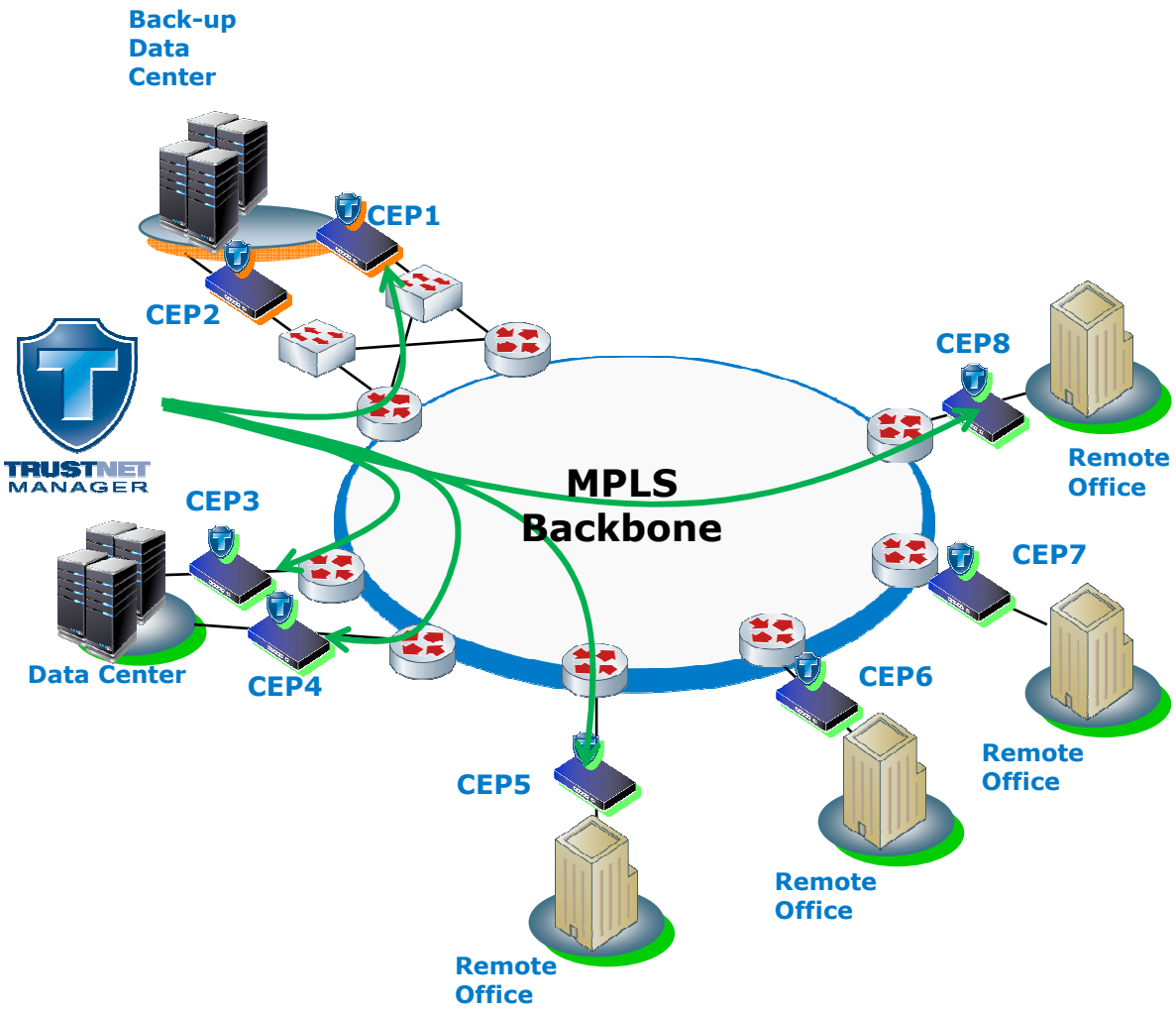


Figure 5: Typical Operational Configuration.

The Crypto Security Officer configures the traffic rules and pushes the resulting policy to the CEP encryptors. In the illustration above, the MPLS backbone is the untrusted network**.** CEPs 1, 2, 3, 4, 5 and 8 are fully meshed, protecting traffic flowing over the MPLS backbone or Internet. The CEP solution is agnostic to the wide area network technology. The MPLS backbone is shown for illustrative purposes, but the network could also be Layer-2 Ethernet using E-LAN (VPLS), a public IP network, Ethernet over DWDM, or a wireless network.

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:

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

2.4.1 Operational Constraints

The 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.

- CEP Installation Guide
- TrustNet Manager User Guide
- CEP CLI 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 CEP must always use FIPS approved encryption and message authentication in security policies as outlined in Section 2.2, Table 3.

The CEP Ethernet management interface must always operate using FIPS-approved cipher/authentication algorithms as outlined in Section 2.2, Table 4. TLS is used for configuration and policy management. SSH is used to secure the command line interface session.

2.5 Secure Setup Procedure

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

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

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

The following software must be installed on the management workstation:

- TrustNet manager 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 web browsers are supported:

- IE, Chrome, FireFox, Safari browsers for TrustNet Manager.

2.5.1 Initiating FIPS Compliant Mode

As stated in Section 2.5, the 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, enable FIPS mode.
2. After the CEP reboots, log in to the CLI as the Crypto Security Officer and set the management port IP address, network mask and network gateway for the module.
3. As the Crypto Security Officer, specify the password enforcement mode to be used for the CEP to choose either the default (described here), or strong. After you have specified the password strength, change the default CEP passwords for both the Crypto-Security Officer and Operator roles. The default CEP passwords must be a minimum of 8 characters and a maximum of 256 characters, and composed of upper and lowercase characters, numeric characters, and special characters (~`!@#%^*_-+={[}]:,.).
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. As the Crypto Security Officer or Ops user, log into the CLI. Obtain the current mode of FIPS operation by entering the command "show fips-mode". The CEP will indicate if the CEP has FIPS mode is enabled, if FIPS mode is operating and if, if FIPS mode is enabled, if FIPS mode is in an error state.

3 Purpose of the CEP Security Policy

CEP encryptors are high performance, integrated encryption appliances that offer full line rate IP Packet and Ethernet Frame encryption for 3 Mbps thru 1Gbps Ethernet transports. Housed in a tamper evident chassis, the

CEPs have two functional Ethernet ports used for traffic. 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 algorithms employed by the CEPs (Section 2.2, Table 3) to encrypt/decrypt/assure message integrity/authenticate all sensitive data include the current standards for the protection of Unclassified but Sensitive Information for the Federal Government.

3.1 CEP Key Management

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

Key Exchange / Key Establishment
Authenticated Diffie-Hellman key exchange (1024 to 4096 bit modulus)
RSA (Key transport)

Key Types

Table 5: Keys and CSPs

Key Name	Description and /or Purpose	Type of Key	Storage Location	Storage Method
Pre-Shared Key	Encryption/Decryption	AES 256 bits	Non-volatile Flash	Plain-text
IKE Pre-Shared Key	Used in L2 IKE negotiation to derive session keys.	20 Character hexadecimal value	Non-volatile Flash	Plain-text
Session Encryption Key	One Symmetric Key per IPSec Security Association (SA) or DistKey (SA)	AES 128 and 256 bits, 168 bits Triple-DES (Distkey only)	Non-volatile Flash	Plain-text
Session Authentication Key	One Authentication Key per IPSec Security Association (SA) or DistKey (SA)	HMAC-SHA-1 (160 bits) and HMAC-SHA-2 (256 bits)	Non-volatile Flash	Plain-text
Management Session Key	Encrypt messages to and from the management tool	256 bits AES and168 bits Triple-DES	Non-volatile Flash	Plain-text
CEP Identification Keys	Authenticate messages to and from the management tool	1024, 1536, 2048, 3072, 4096-bit public/private keys	Non-volatile Flash	Plain-text
Firmware Upgrade Key	Authenticates firmware to be loaded.	HMAC-SHA-2 key (256 bits)	Non-volatile Flash	Plain-text
ANSI X9.31 RNG Seed Key	Used with the ANSI X9.31 RNG	AES 128, 192 or 256 bits	Volatile RAM	Plain-text
ANSI X9.31 RNG Seed	ANSI X9.31 RNG seeding material	128 bit random value taken from 384 bits of seed material	Volatile RAM	Plain-text
SNMPv3 User Authentication Key	This secret is for SNMPv3 authentication and is derived from the SNMPv3 user password.	HMAC-SHA-1 key (160 bits)	Non-volatile Flash	Plain-text
Diffie-Hellman Keys	Used for DH key agreement protocol	1024, 1536, 2048, 3072, 4096-bit public/private	Volatile RAM	Plain-text

Key Name	Description and /or Purpose	Type of Key	Storage Location	Storage Method
		keys		

Zeroization

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

3.2 Module Self-Tests

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

Power-Up Tests:

Cryptographic Implementations (Hardware):

Triple DES KAT
AES KAT
HMAC-SHA-1 KAT
HMAC-SHA-2 KAT

Certes Networks CEP Cryptographic Library #1 (Firmware):

Triple-DES KAT
AES KAT
SHA-1 KAT
SHA-256 KAT
SHA-512 KAT
HMAC-SHA-1 KAT
HMAC-SHA-224 KAT
HMAC-SHA-256 KAT
HMAC-SHA-384 KAT
HMAC-SHA-512 KAT
RNG (ANSI X9.31) KAT
DSA KAT
RSA KAT

Firmware Integrity Test (Verification of SHA-1 digest)

Continuous Random Number Generator Test:

The CEP includes a continuous test on the output from the FIPS compliant RNGs 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 CEP includes a conditional pairwise consistency test (sign and verify operation) every time RSA and DSA keys are generated.

Conditional Bypass Test:
The CEP includes a conditional bypass test that is performed prior to loading any file containing policies, keys, or configurations. The conditional bypass test performs a SHA-1 hash verification that each file contents have not changed or been corrupted.

Firmware Load Test:

The 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 enters an error state and all the data ports are 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.

Manual Key Entry Test

When the use enters performs manual entry of pre-shared policy keys via the CLI, the keys must be separately entered two times. These entries are compared to verify matching entry and are checked to ensure correctness of the data entry (such as key size). If either test fails the key entry is rejected.

4 Specification of the CEPS Security Policy

4.1 Roles

Three roles, which either provide security services or receive services of the CEP, are the basis of the specification of the 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 CEP by maintaining all identity-based user id/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 CEP. The Network User is any CEP that is authenticated with another CEP to perform encryption and decryption services. The 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 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 entity is uniquely identified with a user ID and password/key. With the minimum password length of 8 characters, 81 available characters, and a minimum 1 second delay between failed login attempts, the probability of guessing a password in 1 minute is $1/ (3.0 * 10^{13})$. For the strong password enforcement, the minimum password length is 15 characters and the probability of guessing the password in 1 minute with a 1 second delay between attempts is $1/ (7.1 * 10^{26})$.

Table 6: Identification/Authentication Policy

Role	Identification/ Authentication	Strength of Authentication
Operator (OPS)	Ops UserId/Password	Default: $1/ (3.0 * 10^{13})$ Strong:$1/ (7.1 * 10^{26})$
Crypto Security Officer (CSO)	Admin UserId/Password	Default: $1/ (3.0 * 10^{13})$ Strong:$1/ (7.1 * 10^{26})$
Network User (User)	Session authentication key/20 byte HMAC-SHA-1, 32 Byte HMAC-SHA-2	$1: 10^{24}$

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 6.

4.3 Access Control, Roles, and Services

Table 7 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 CEP module (exclusive of the dual power supplies) 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 7: 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	**Set Password Policy**		
	Define the policy for the Ops and Admin passwords.	Password	Write, Execute
CSO	**Change Passwords**		
	Change the Ops and Admin passwords.	Password	Write, Execute
CSO	**View Audit Log**		
	Views the audit-log information.	None	Read
CSO	**Zeroization**		
	Zeroize the CEP. The CSO must maintain control of the CEP during the process of zeroization to ensure no unauthorized access could occur before zeroization is complete.	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. OPS: Configure date/time, disable trusted hosts, clear known hosts, configure management port IP address, mask, and gateway.	None	Read, Write, Execute
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,	None	Read

Roles	CEP Services	Security Relevant Data Item	SRDI Access Read, Write, Execute
	security policy information (SAD and SPD).		
CSO OPS	**Reboot**		
	Reboot the CEP.	None	Execute
CSO OPS	**Restart**		
	Restart the CEP management software without full system reset.	None	Execute
CSO	**Edit Security Policy**		
	Update the security policy rules of the CEP.	Triple DES, AES, RSA	Read, Write
CSO	**Load Security Policy**		
	Load an updated or saved security policy into the CEP.	None	Execute
CSO	**Delete Security Policy**		
	Delete a security policy in the CEP.	None	Execute
CSO	**Firmware Upgrade**		
	Update the firmware of the CEP.	HMAC-SHA-256	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 CEP has been designed 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 on CEP100-XSA, CEP1000, CEP1000-DP, CEP1000 VSE and not present on CEP100 and CEP100 VSE), as well as the RS-232 serial port, 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 at manufacturing 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).

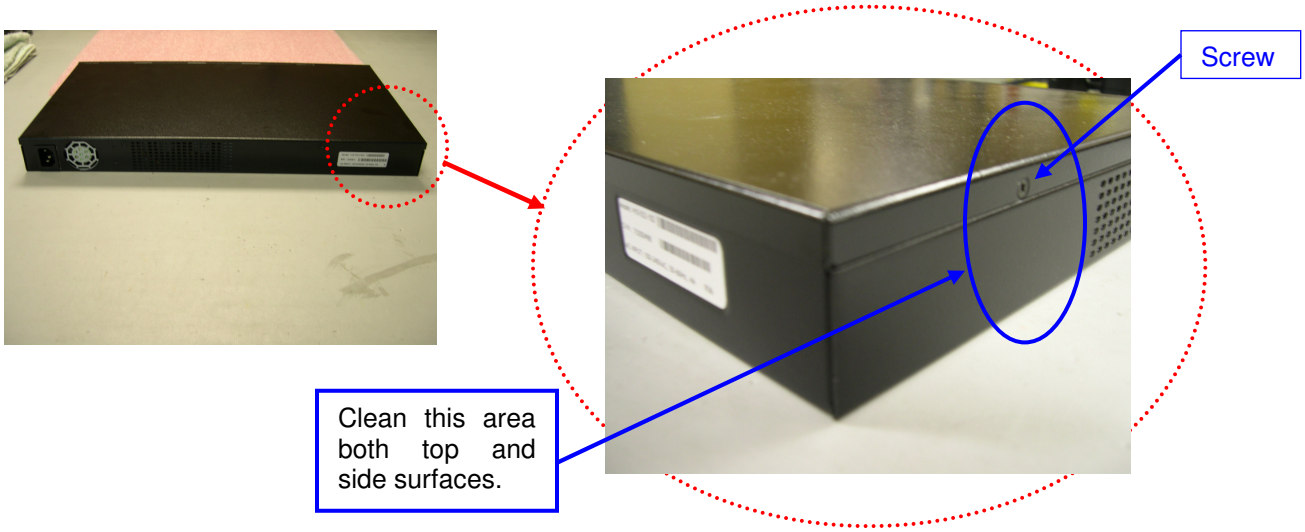
The Crypto Security Officer shall periodically check the tamper evident seal to verify that the module has not been opened. If the seal is broken, the unit should be removed from service and a replacement unit obtained from the vendor.

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

At the factory the serialized tamper evident seal shall be applied as follows::

1. Turn off and unplug the CEP before cleaning the CEP and applying labels.
2. Clean the CEP of any grease, dirt or oil before applying the tamper evident labels. . For optimum adhesion, surfaces must be cleaned with isopropyl alcohol (99%) to remove any surface contaminants before affixing label. See photo below for cleaning area.

Figure 7. Area to clean for application of tamper evident label.



3. Identify the location to attach the label. Take note of the location of the screw head and the small hole. The label spans across rear and top panels, completely covering screw head. Note: Ventilation holes are not covered by label as shown. The minimum temperature for application is +50F.

Figure 8. Tamper evident label placement location.

4. Remove the label from the roll. Minimize contact with the label by using tweezers or a knife. If the label adhesive touches anything before application and comes off or is contaminated, the label must be discarded and a new one used.
5. Apply the label in the identified location ensuring the screw head is covered and the top and rear panels are spanned.
6. Allow the label to cure 48 hours to ensure the adhesive is firmly affixed.
7. Record the label serial number and void any record of the discarded label serial number.

4.5 Strength of Function

Within the cryptographic security boundary, the 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 CEP's network address will be discarded. 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

Table 8: Access Interfaces and Role Permissions for Services.

Service	Access Interface		Role Permissions		
	CLI	XML/RPC	CSO	OPS	User
Create Users	✓	✓	✓		
Set Password Policy	✓	✓	✓		

Service	Access Interface		Role Permissions		
	CLI	XML/RPC	CSO	OPS	User
Change Passwords	✓	✓	✓		
Set Audit Log		✓	✓		
View Audit Log	✓	✓	✓		
Zeroization	✓		✓		
Run Self-Test	✓	✓	✓	✓	
Key Generation	✓	✓	✓		
Configure	✓	✓	✓	✓	
Enable FIPS Mode	✓	✓	✓		
Create Security Policy	✓	✓	✓		
Show Status	✓	✓	✓	✓	
Reboot	✓	✓	✓	✓	
Restart	✓		✓	✓	
Edit Security Policy	✓	✓	✓		
Load Security Policy	✓	✓	✓		
Delete Security Policy	✓	✓	✓		
Firmware Upgrade	✓	✓	✓		
Key Establishment		✓	✓		
Restore-File system	✓	✓	✓		
Shutdown	✓	✓	✓	✓	
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 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.

Distkey

Keys and policies are distributed from the management application to the CEP modules using TLS 1.0.d

Network User (User)

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

KAT

Known Answer Test used in verifying the correct operation of a cryptographic algorithm

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 CEP are operated in a safe and effective manner. The CEP Security Policy shall be applied to all Ethernet or IP data flows through the 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.

VSE

Variable Speed Encryptor. The CEP VSE is capable of transmitting traffic at a range of speeds that varies by hardware model. Throughput speed is controlled with a license.

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”

CEP VSE-series Installation Guide, Version 2.1

CEP VSE-series CLI User Guide, Version 2.1

TrustNet Manager User Guide, Version 3.2

CEP FIPS 140-2 Vendor Evidence Document, January, 2012

Finite State Machine Document, January, 2012

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		
B	Updated for CEP 1.6 and VSE		
C	Updated for CEP 2.1		
D	Updated after CEP 2.1 Reviews. Update figure/table labels.		
E	Updates from Review		