Security Policy

CLE- T3 Link Encryptor

(version 3.00, h/w Rev 3)

ES-16758-4

November 27, 2001

Prepared by

CYLINK CORPORATION

1 Scope of Document

This document contains the security policy requirements for the Cylink CLE- T3 Link Encryptor system module. The CLE- T3 Link Encryptor System shall be referred to as the CLE (Cylink Link Encryptor) in this document.

2 Applicable Documents

• FIPS 140-1	Security Requirements for Cryptographic Modules
• DTR	Derived Test Requirements for FIPS 140-1, Security Requirements for Cryptographic Modules (DTR)
• FIPS 46-2	Data Encryption Standard (DES)
• FIPS 81	DES Modes of Operation
• FIPS 180-1	Secure Hash Standard (SHA-1)
• FIPS 186	Digital Signature Standard (DSS)

3 Security Level

The CLE meets the overall requirements applicable to Level 2 security of FIPS 140-1, and meets Physical Security and Software Security applicable to Level 3.

Security Requirements Section	Level
Cryptographic Module	2
Module Interfaces	2
Roles and Services	2
Finite State Machine	2
Physical Security	3
EFP/EFT	N/A
Software Security	3
Operating System Security	N/A
Key Management	2
Cryptographic Algorithms	2
EMI/EMC	2
Self Test	2

4 Security Rules

This section documents the security rules enforced by the CLE to implement the security requirements of FIPS 140-1 overall Level 2 module, with Level 3 Software and Physical Security.

4.1 Cryptographic Module

The CLE shall be implemented as a “Multiple-Chip Standalone Cryptographic Module” as defined in FIPS 140-1.

4.2 Roles and Services

The CLE shall employ role based authentication of the operator. The module supports two roles as required by FIPS 140-1. The roles are the User Role and the Crypto Officer Role. The User Role is restricted to viewing status and alarms, while the Crypto Officer role provides full privileges for mode control, device configuration, and test functions. Access to the Crypto Officer role is restricted at the front panel by the use of a Medeco lock, and at the Network Management (ethernet) port by the verification (by the CLE and the network application, Privacy Manager) of mutually authenticated Cylink manufacturing certificates.

The Privacy Manager is a separate product, and contains its own methods for establishing and validating roles, which may be restricted to subset of those supported by the CLE. Additionally, PrivaCy Manager can initiate network/voice authentication, initiate a software download operation, display the CLE MAC address, and display the date and time of the last key exchange. PrivaCy Manager is not part of the cryptographic module validation for the CLE-T3.

An operator is authenticated to the Crypto Officer role at the front panel through possession of the key that will turn the Medeco lock to the Enable position. Concurrent operator access/operation is prevented by disallowing SNMP access (from Privacy Manager) when the Medeco lock is set to enable the front panel.

Physical Maintenance shall be performed at the factory, as there are no services that require the cover to be removed in the field, and there are no logical maintenance services performed in the field. The CLE module should be zeriozed by a Crypto Officer before the module is returned to the factory, either by command or by removing the cover.

4.2.1 User Role

The User Role provides the operator with the ability to view the operational mode of the CLE and also to view outstanding alarms.

4.2.2 Crypto Officer Role

The Crypto Officer Role provides the operator the ability to perform all of the services listed below.

1. Set Operational Mode: This service allows the operator to select the current operational mode. The operator shall be permitted to command the CLE into the following modes:

   a) Clear Mode
   b) Standby Mode
   c) Secure Mode

2. Alarm/Event Services

   a) Display Event Log: This service allows the operator to scroll through and view the contents of the CLE's event log.

   b) Clear Event Log: This service allows the operator to completely clear the contents of the event log.

3. Time/Date: This service allows the operator to set the real time clock to the current date and time.

4. Key Management

   a) Set Auto Key Change Attributes

   b) Days Interval

   c) End to End Delay

   d) Clear Modes Allowed/Disallowed

   e) Mode NET CERT, MANUAL (authentication) KEY, UNAUTH DH

   f) Zeroize Keys: This service allows the operator to erase **critical** security parameters. When this service is activated the following information shall be actively erased:

      (i) CLE Network Certificate

      (ii) CLE DSS secret key (X)

      (iii) PrivaCy Manager DSS public key

      (iv) PrivaCy Manger/CLE (SNMP) encryption key

      (v) PrivaCy Manger/CLE SNMP message counter

      (vi) CLE/CLE encryption key

      (vii) Manually Entered Authentication Key

      (viii) Far End CLE serial number

      (ix) Last key change timestamp

      (x) Event Log

   g) Set Manual Authentication Key

   h) Adapt Algorithm Allowed/Disallowed

5. Network Management

   a) Display/Set Unit IP Address

b) Display/Set Gateway IP Address

c) Display/Set Subnet Mask Address

d) Display/Set Trap1/Trap2 IP Address

6. System Test: This service allows the operator to set a Network Encryptor Loopback, or a DTE Encryptor Loopback, or clear a loopback that has been previously set. CLEs with a T1, E1, or T3 interface also allow setting or clearing a Network Line Loopback or a DTE Line Loopback. The T3 encryptor also allows the operator to set or clear a Bit Error Rate Test (BERT).
7. Display Manufacturing Info: This service allows the operator to display the following information:

a) Firmware Revision

b) Firmware Date

c) Hardware List

d) Hardware Issue

e) Manufacturing Date

f) Unit Serial Number

g) Line Interface Unit (LIU) Type

h) Daughterboard firmware version (T3 only)

i) End to End (Link) Key Size, and Encryption Mode and Algorithm

j) SNMP Key Size, and Encryption Mode and Algorithm

8. Set Default Configuration
9. Firmware Update

4.3 Physical Security

1. Tamper evident tape spans the interface between the removable cover assembly and the chassis rear. It is not possible to remove the enclosure cover without destroying the tamper evident tape. Operation of the front panel user interface is restricted by the use of a Medeco lock. The purpose of this lock is not to prevent opening the unit.
2. The CLE includes tamper response and zeroization circuitry. Upon the removal of the enclosure's cover, all plaintext cryptographic key and unprotected critical security parameters are immediately zeroized. This capability is operational whether or not power is applied to the module.
3. CLE-T3 operates on 110 V AC only, and does not require a fan for cooling and therefore does not use ventilation holes. Thus internal baffles to prevent physical probing inside the enclosure are not required and are not part of the design.
4. The CLE-T3 is made of commercially available, production grade componenets. All integrated circuit chips have passivation applied to them.

4.4 Operating System Security

The FIPS 140-1 operating system requirements (FIPS PUB 140-1 section 4.7) do not apply to the CLE because it is not a general purpose computer and thus it cannot run untrusted user-supplied software. However, the CLE’s firmware can be field updated using a download process. The following rules apply to the downloading of new CLE firmware.

The CLE shall verify the signature of the binary image. If this verification fails, the module shall continue operation using the pervious version of firmware, the downloaded binary image shall be marked as non-executable, and an SNMP-readable MIB status shall be set reporting the failure.

For CLE-T3 only, there is also firmware resident in flash memory on the daughter board. This firmware can also be updated via the same download process, with the same verification steps as is the case for the main board firmware.

4.5 Key Management

1. The PRNG seed (referred to as the XKEY in FIPS 186 Appendix 3.1) shall be installed into the CLE using the Cylink Manufacturing Configurator (CMC) process.
2. PrivaCy Manager/CLE encryption keys shall be re-negotiated each time a new CLE Network Certificate is loaded.
3. PrivaCy Manager/CLE encryption keys shall be established using the Diffie-Hellman Key Agreement process.
4. Messages exchanged between the PrivaCy Manager and the CLE systems that contain the Diffie-Hellman public components used to establish the PrivaCy Manager/CLE encryption key shall be signed using the DSA associated with each entities Manufacturing Certificate.
5. Prior to accepting the PrivaCy Manager/CLE encryption key the CLE shall perform various message and certificate signature verification tests.

   If any of the tests fail the PrivaCy Manager/CLE encryption key and the newly loaded Network Certificate are rejected and the CLE shall report the failure at the end of the protocol.
6. A new CLE/CLE encryption key shall be negotiated each time the CLE transitions from a non-secure state to a secure state.
7. While in the secure mode the CLE/CLE encryption key shall be periodically re-negotiated.
8. CLE/CLE encryption keys shall be established using the Diffie-Hellman Key Agreement process.
9. When establishing a new CLE/CLE encryption key, the messages containing the Diffie-Hellman public component shall be signed.
10. Prior to accepting the CLE/CLE encryption key each CLE shall:

    a) Verify the compatibility of the two units’ session settings:

b) Verify the validity of the Network Certificate's signature.

If any of the above tests fail the CLE/CLE encryption key shall be rejected.

11. If the Leased Line link encryption key generation process fails, the CLE shall generate an alarm.
12. If a successful Leased Line CLE/CLE key exchange does not occur within the Days Interval setting of the previous key exchange, the CLE shall produce an alarm due to the resulting Local Secure mode.
13. The CLE shall have the ability to generate a pseudo-random authentication key, and use it to authenticate the end-to-end communication protocol, in situations where PrivaCy Manger and Network Certificates are not available. The plaintext 24-byte authentication key shall be generated randomly as per FIPS Pub 186, shall not be displayed after user acceptance, and shall be zeroized by operator command or by a tamper situation.
14. The CLE shall have the ability to accept and utilize a manually entered end-to-end authentication key. The plaintext 24-byte authentication key shall not be displayed after user entry, and shall be zeroized by operator command or by a tamper situation.
15. All persistent keys shall be stored in tamper-protected non-volatile memory in clear text.

4.6 Crypto Algorithms

1. The CLE shall use the Triple Data Encryption Standard (TDES) algorithm to protect the user line data. Sensitive PrivaCy Manager/CLE data shall be protected using the Triple DES algorithm.
2. The CLE shall use the Digital Signature Standard as described in FIPS 186 for the authentication of all security related information.
3. As specified in FIPS 186, the module will also support the Secure Hash Standard (SHA-1) as described in FIPS 180-1.

4.7 Self Test

1. The following Power-Up Self Tests shall be performed when power is first applied to the system.

a) Field Programmable Gate Array (FPGA) Test

b) Program Memory (ROM/FLASH) Integrity Test

c) Bypass Test

d) General Purpose Memory Test

e) Non-Volatile Memory Integrity Test

f) Real Time Clock Test

g) Cipher Chip Test

h) Random Number Generator Test

i) General Cryptographic Algorithm Test

j) Pair wise Consistency Test

2. During normal operation, once during each second the battery that backs up the non-volatile RAM shall be tested.
3. All keys to be used for symmetric key cryptographic algorithms shall be checked to verify that they are cryptographically suitable for use as an encryption/decryption key. This check shall be performed immediately after the value of the key has been established.

   For example, a DES key must be checked to verify that it is of the correct parity and is not on the list of known “weak” or “semi-weak” DES keys.

5 Definition of Security Relevant Data Items (SRDIs)

(1) CLE Manufacturing Certificate

(2) PrivaCy Manager Manufacturing Certificate

(3) PrivaCy Manager/CLE SNMP Encryption Algorithm Flag

(4) PrivaCy Manager/CLE SNMP Encryption Mode Flag

(5) PrivaCy Manager/CLE SNMP Encryption Key Size Flag

(6) CLE to CLE Encryption Algorithm Flag

(7) CLE to CLE Encryption Mode Flag

(8) CLE to CLE Encryption Key Size Flag

(9) Near End Network Certificate

(10) Far End Network Certificate

(11) Far End Manual Authentication Code

(12) Firmware Binary Image Signature

(13) PRNG Running Seed (XKEY)

(14) CLE DSS Secret Key (X)

(15) CLE DSS Public Key (Y)

(16) PrivaCy Manager DSS Public Key

(17) PrivaCy Manager/CLE (SNMP) Encryption Key

(18) PM/CLE Message Counter Value

(19) PrivaCy Manager/CLE Message Counter

(20) CLE/CLE Encryption Key

(21) Near End CLE Challenge Value

(22) Far End CLE Challenge Value

(23) Voice Authentication Hash Value

(24) Far End CLE Serial Number

(25) Far End CLE Serial Number timestamp

(26) Last Key Change Timestamp

(27) Event Log

(28) Key Change Method

(29) Begin Time

(30) End Time

(31) Days Interval

(32) Clear Modes

(33) Key Management Mode

(34) Manual Authentication Key

(35) Algorithm Adaptation Flag

(36) Exclusion List: For Dial-Up operation

6 Definitions of SRDI Modes of Access

The table below defines the relationship between access to SRDIs and the different module services. The modes of access are shown as codes in the table and are defined as follows:

a) **D** - The SRDI is set back to the manufacturing default by the service.
b) **G** - This service generates the SRDI internal to the CLE.
c) **I** - The SRDI is input into the CLE by this service.
d) **R** - The SRDI is read and used by the service.
e) **U** - The SRDI is updated by the service.
f) **V** - The SRDI is verified by the service.
g) **Z** - The SRDI is erased by the service.

Table 1 Services Versus SRDI Access

Manufacturing Service and User/Crypto Officer Service	Security Relevant Data Items (PM=PrivaCy Manager, CLE=Cylink Link Encryptor)																														Role	
	CLE Manufacturing Certificate	PM Manufacturing Certificate	PM/CLE Encrypt Algo Flag	PM/CLE Encrypt Mode Flag	PM/CLE Encrypt Key Size Flag	CLE/CLE Encrypt Algo Flag	CLE/CLE Encrypt Mode Flag	CLE/CLE Encrypt Key Size Flag	Near End CLE Network Certificate	Far End CLE Network Certificate	PRNG Running Seed (XKEY)	CLE DSS Secret Key (X)	CLE DSS Public Key (Y)	PM DSS Public Key	PM/CLE Encryption Key	PM/CLE Challenge Value	PM/CLE Message Counter	CLE/CLE Encryption Key	Near End CLE Challenge Value	Far End CLE Challenge Value	Voice Authentication Hash Value	Far End CLE Serial Number	Last Key Change Timestamp	Event Log	Key Change Method	Begin Time	End Time	Days Interval	Clear Modes Allow/Disallow	Mode Managed/Unmanaged	User Role	Crypto Officer Role
Manufacturing CMC			I	I	I	I	I	I			I																					
Manufacturing CCA	I											G	G																			
Perform Network Authentication	V	IV							GV			R	R	I	G	V	U															X
Renewal of Network Authentication									GV			R	R	I	G	V																X
Perform PM/CLE Voice Authentication									GV			G	G	I	G	V	U				GV											X
Set Operational Mode - Clear										V									G	V		U		U					R			X
Set Operational Mode - Standby										V									G	V		U		U								X
Set Operational Mode - Secure			R	R	R	R	R	R		V	U							G	G	V		U	U	U						R		X
Display Event Log																								R								X
Reset Event Log																								Z								X
Set Time/Date																																X
Set Key Change Method																									RI							X
Set Begin Time																										RI						X
Set End Time																											RI					X
Set Days Interval																												RI				X
Set End-to-End Delay																																X
Set Clear Modes Allow/Disallow																													RI			X
Set Mode Managed/Unmanaged																														RI		X
Zeroize Keys									Z			Z		Z	Z		Z	Z				Z	Z	Z								X
Set Line Interface Parameters																																X
Set CLE IP Address																																X
Set Gateway IP Address																																X
Set Subnet Mask																																X
Set Trap1 IP Address																																X
Set Trap2 IP Address																																X
Display System Info			R	R	R	R	R	R																								X
Set/Clear DTE/NET Loopbacks																																X
Set Default Configuration																						D	D		D	D	D	D	D	D		X
PM User Role Services																																
View Operational Mode																															X	
View Alarm Status																															X	
View Trap Information																															X	
View Trap Forwarding Parameters																															X	
View Event Browser.																															X	
View Communication Parameters																															X	
View Audit Log																															X	
View Login Parameters																															X	
Change Users Own Password and Login Properties																															X	
Print Security Policy Report																															X	
Print Inventory Report																															X	
Locate Module by Name																															X	
Locate Module by IP																															X	