

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31

Security Policy

For

NRZ/T1/E1 Link Encryptor

ES-14885-4
Rev B

May 17, 1999

Prepared by

CYLINK CORPORATION

1			
2	1	SCOPE OF DOCUMENT	2
3	2	APPLICABLE DOCUMENTS	2
4	3	SECURITY LEVEL	3
5	4	SECURITY RULES	3
6	4.1	CRYPTOGRAPHIC MODULE	4
7	4.2	ROLES AND SERVICES.....	4
8	4.2.1	<i>User Role</i>	4
9	4.2.2	<i>Crypto Officer Role</i>	5
10	4.3	PHYSICAL SECURITY	6
11	4.4	OPERATING SYSTEM SECURITY	6
12	4.5	KEY MANAGEMENT	7
13	4.6	CRYPTO ALGORITHMS	8
14	4.7	SELF TEST	8
15	5	DEFINITION OF SECURITY RELEVANT DATA ITEMS (SRDIS)	9
16	6	DEFINITIONS OF SRDI MODES OF ACCESS	10

17

18 1 Scope of Document

19

20 This document contains the security policy requirements for the Cylink NRZ/T1/E1 Link
 21 Encryptor system module. The NRZ/T1/E1 Link Encryptor System shall be referred to as the
 22 CLE (Cylink Link Encryptor) in this document.

23

24 2 Applicable Documents

25

- 26 • FIPS 140-1 Security Requirements for Cryptographic Modules
- 27 • DTR Derived Test Requirements for FIPS 140-1, Security Requirements
 28 for Cryptographic Modules (DTR)
- 29 • FIPS 46-2 Data Encryption Standard (DES)
- 30 • FIPS 81 DES Modes of Operation
- 31 • FIPS 180-1 Secure Hash Standard (SHA-1)
- 32 • 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 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. Access to these roles is restricted at the front panel by the use of a Medeco lock, and at the Network Management (ethernet) port by the use of a password entered into the PrivaCy Manager system. An operator is authenticated to the User and Crypto Officer roles 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 when the Medeco lock is set to enable the front panel.

PrivaCy Manager is an application that can be used to remotely control the CLE through an Ethernet connection. In addition to the services that can be initiated from the front panel, 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.

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 zeroized 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 control the operational mode of the CLE and thus configure the network security policy. The services available to an operator while in the User Role are as follows:

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
 - d) Clear Pending Secure Mode (Dial-Up only)
 - e) Standby Pending Secure Mode (Dial-Up only)

4.2.2 Crypto Officer Role

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

1. 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.
- f) Clear Event Log: This service allows the operator to completely clear the contents of the event log.

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

3. 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

4. Set Line Interface Configuration Parameters

5. Network Management

- a) Display/Set Unit IP Address
- b) Display/Set Gateway IP Address

- 1 c) Display/Set Subnet Mask Address
2 d) Display/Set Trap1/Trap2 IP Address
3 6. System Test: This service allows the operator to set a Network Encryptor Loopback, or
4 a DTE Encryptor Loopback, or clear a loopback that has been previously set. CLEs
5 with a T1 or E1 interface also allow setting or clearing a Network Line Loopback or a
6 DTE Line Loopback
7 7. Display Manufacturing Info: This service allows the operator to display the following
8 information:
9 a) Firmware Revision
10 b) Firmware Date
11 c) Hardware List
12 d) Hardware Issue
13 e) Manufacturing Date
14 f) Unit Serial Number
15 g) Line Interface Unit (LIU) Type
16 h) End to End (Link) Key Size, and Encryption Mode and Algorithm
17 i) SNMP Key Size, and Encryption Mode and Algorithm
18 8. Set Default Configuration
19 9. Firmware Update
20

21 4.3 Physical Security

- 22
23 1. Access to the circuitry contained within the CLE shall be restricted by the use of a
24 Medeco lock. It shall not be possible to remove the enclosure cover without unlocking
25 the lock.
26 2. The CLE shall include tamper response and zeroization circuitry. Upon the removal of
27 the enclosure's cover, all plaintext cryptographic key and unprotected critical security
28 parameters shall be immediately zeroized. This capability shall be operational whether
29 or not power is applied to the module.
30 3. The CLE shall not employ ventilation holes, and shall be designed to prevent physical
31 probing inside the enclosure.
32
33

34 4.4 Operating System Security

35

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

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

10 4.5 Key Management

- 11
- 12 1. The PRNG seed (referred to as the XKEY in FIPS 186 Appendix 3.1) shall be installed
- 13 into the CLE using the Cylink Manufacturing Configurator (CMC) process.
- 14 2. PrivaCy Manager/CLE encryption keys shall be re-negotiated each time a new CLE
- 15 Network Certificate is loaded.
- 16 3. PrivaCy Manager/CLE encryption keys shall be established using the Diffie-Hellman
- 17 Key Agreement process.
- 18 4. Messages exchanged between the PrivaCy Manager and the CLE systems that contain
- 19 the Diffie-Hellman public components used to establish the PrivaCy Manager/CLE
- 20 encryption key shall be signed using the DSA associated with each entities
- 21 Manufacturing Certificate.
- 22 5. Prior to accepting the PrivaCy Manager/CLE encryption key the CLE shall perform
- 23 various message and certificate signature verification tests.
- 24 If any of the tests fail the PrivaCy Manager/CLE encryption key and the newly loaded
- 25 Network Certificate are rejected and the CLE shall report the failure at the end of the
- 26 protocol.
- 27 6. A new CLE/CLE encryption key shall be negotiated each time the CLE transitions from
- 28 a non-secure state to a secure state.
- 29 7. While in the secure mode the CLE/CLE encryption key shall be periodically re-
- 30 negotiated.
- 31 8. CLE/CLE encryption keys shall be established using the Diffie-Hellman Key Agreement
- 32 process.
- 33 9. When establishing a new CLE/CLE encryption key, the messages containing the Diffie-
- 34 Hellman public component shall be signed.
- 35 10. Prior to accepting the CLE/CLE encryption key each CLE shall:
- 36 a) Verify the compatibility of the two units' session settings;
- 37 b) Verify the validity of the Network Certificate's signature.
- 38 If any of the above tests fail the CLE/CLE encryption key shall be rejected.
- 39

1 11. If the Leased Line link encryption key generation process fails, the CLE shall generate
2 an alarm.

3 12. If a successful Leased Line CLE/CLE key exchange does not occur within the Days
4 Interval setting of the previous key exchange, the CLE shall produce an alarm due to
5 the resulting Local Secure mode.

6 13. The CLE shall have the ability to generate a pseudo-random authentication key, and
7 use it to authenticate the end-to-end communication protocol, in situations where
8 PrivaCy Manger and Network Certificates are not available. The plaintext 24-byte
9 authentication key shall be generated randomly as per FIPS Pub 186, shall not be
10 displayed after user acceptance, and shall be zeroized by operator command or by a
11 tamper situation.

12 14. The CLE shall have the ability to accept and utilize a manually entered end-to-end
13 authentication key. The plaintext 24-byte authentication key shall not be displayed after
14 user entry, and shall be zeroized by operator command or by a tamper situation.

15 16 **4.6 Crypto Algorithms**

- 17
- 18 1. The CLE shall use the Data Encryption Standard (DES) algorithm or Triple DES to
19 protect the user line data. Sensitive PrivaCy Manager/CLE data shall be protected
20 using the Triple DES algorithm.
 - 21 2. The CLE shall use the Digital Signature Standard as described in FIPS 186 for the
22 authentication of all security related information.
 - 23 3. As specified in FIPS 186, the module will also support the Secure Hash Standard
24 (SHA-1) as described in FIPS 180-1.

25 26 **4.7 Self Test**

- 27
- 28 1. The following Power-Up Self Tests shall be performed when power is first applied to the
29 system.
 - 30 a) Field Programmable Gate Array (FPGA) Test
 - 31 b) Program Memory (ROM/FLASH) Integrity Test
 - 32 c) General Purpose Memory Test
 - 33 d) Non-Volatile Memory Integrity Test
 - 34 e) Real Time Clock Test
 - 35 f) Cipher Chip Test
 - 36 g) Random Number Generator Test
 - 37 h) General Cryptographic Algorithm Test

1 i) Pairwise Consistency Test

2
3 2. During normal operation, once during each second the battery that backs up the non-
4 volatile RAM shall be tested.

5 3. All keys to be used for symmetric key cryptographic algorithms shall be checked to
6 verify that they are cryptographically suitable for use as an encryption/decryption key.
7 This check shall be performed immediately after the value of the key has been
8 established and before the key is used or stored for later use.

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

11 **5 Definition of Security Relevant Data Items (SRDIs)**

- 12
13 (1) CLE Manufacturing Certificate
14 (2) PrivaCy Manager Manufacturing Certificate
15 (3) PrivaCy Manager/CLE SNMP Encryption Algorithm Flag
16 (4) PrivaCy Manager/CLE SNMP Encryption Mode Flag
17 (5) PrivaCy Manager/CLE SNMP Encryption Key Size Flag
18 (6) CLE to CLE Encryption Algorithm Flag
19 (7) CLE to CLE Encryption Mode Flag
20 (8) CLE to CLE Encryption Key Size Flag
21 (9) Near End Network Certificate
22 (10) Far End Network Certificate
23 (11) Far End Manual Authentication Code
24 (12) Firmware Binary Image Signature
25 (13) PRNG Running Seed (XKEY)
26 (14) CLE DSS Secret Key (X)
27 (15) CLE DSS Public Key (Y)
28 (16) PrivaCy Manager DSS Public Key
29 (17) PrivaCy Manager/CLE (SNMP) Encryption Key
30 (18) PM/CLE Message Counter Value
31 (19) PrivaCy Manager/CLE Message Counter
32 (20) CLE/CLE Encryption Key
33 (21) Near End CLE Challenge Value
34 (22) Far End CLE Challenge Value

- 1 (23) Voice Authentication Hash Value
- 2 (24) Far End CLE Serial Number
- 3 (25) Far End CLE Serial Number timestamp
- 4 (26) Last Key Change Timestamp
- 5 (27) Event Log
- 6 (28) Key Change Method
- 7 (29) Begin Time
- 8 (30) End Time
- 9 (31) Days Interval
- 10 (32) Clear Modes
- 11 (33) Key Management Mode
- 12 (34) Manual Authentication Key
- 13 (35) Algorithm Adaptation Flag
- 14 (36) Exclusion List: For Dial-Up operation
- 15

16 6 Definitions of SRDI Modes of Access

17

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

20

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

Table 1 Services Versus SRDI Access

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	Far End Manual Auth Code	Firmware Binary Image Signature	FRNG 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	Key Management Mode	Manual Authentication Key	Algorithm Adaptation Flag	Excursion List	User Role	Crypto Officer Role																				
Manufacturing Service and User/Crypto Officer Service	V	IV																																																							
Perform Network Authentication																																																									
Renewal of Network Authentication																																																									
Perform PM/CLE Voice Authentication																																																									
Set Operational Mode - Clear																																																									
Set Operational Mode - Standby																																																									
Set Operational Mode - Secure																																																									
Display Event Log																																																									
Reset Event Log																																																									
Set Time/Date																																																									
Set Key Change Method																																																									
Set Begin Time																																																									
Set End Time																																																									
Set Days Interval																																																									
Set End-to-End Delay																																																									
Set Clear Modes Allow/Disallow																																																									
Set Key Management Mode																																																									
Zeroize Keys																																																									
Set Manual Authentication Key																																																									
Set Algorithm Adaptation																																																									
Set Line Interface Parameters																																																									
Set Dial-Up Config																																																									
Set CLE IP Address																																																									
Set Gateway IP Address																																																									
Set Subnet Mask																																																									
Set 8 Trap IP Addresses																																																									
Display System Info																																																									
Set/Clear DTE/NET Loopbacks																																																									
Set Default Configuration																																																									
Trigger Firmware Update																																																									