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 Link Encryptor

ES-14885-4
Rev B

May 17, 1999

Prepared by

CYLINK CORPORATION

17

18 1   Scope of Document

19

20 This document contains the security policy requirements for the Cylink NRZ Link Encryptor
21 system module. The NRZ/T1/E1/RS-232 Link Encryptor System shall be referred to as the CLE
22 (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)

1
3 **Security Level**

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

7
8
9
4 **Security Rules**

11
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 Physical Security and
Software Security.

1

4.1 Cryptographic Module

3

4 The CLE shall be implemented as a "Multiple-Chip Standalone Cryptographic Module" as
5 defined in FIPS 140-1.

6

4.2 Roles and Services

8
9 The CLE shall employ role based authentication of the operator. The module supports two
10 roles as required by FIPS 140-1. The roles are the User Role and the Crypto Officer Role.
11 Access to these roles is restricted at the front panel by the use of a Medeco lock, and at the
12 Network Management (ethernet) port by the use of a password entered into the PrivaCy
13 Manager system. An operator is authenticated to the User and Crypto Officer roles at the front
14 panel through possession of the key that will turn the Medeco lock to the Enable position.
15 Concurrent operator access/operation is prevented by disallowing SNMP access when the
16 Medeco lock is set to enable the front panel.

17
18 PrivaCy Manager is an application that can be used to remotely control the CLE through an
19 Ethernet connection. In addition to the services that can be initiated from the front panel,
20 PrivaCy Manager can initiate network/voice authentication, initiate a software download
21 operation, display the CLE MAC address, and display the date and time of the last key
22 exchange.

23
24 Physical Maintenance shall be performed at the factory, as there are no services that require
25 the cover to be removed in the field, and there are no logical maintenance services performed
26 in the field. The CLE module should be zeriozed by a Crypto Officer before the module is
27 returned to the factory, either by command or by removing the cover.

28
29
30 4.2.1 User Role

31
32 The User Role provides the operator with the ability to control the operational mode of the CLE
33 and thus configure the network security policy. The services available to an operator while in
34 the User Role are as follows:

35
36   1. Set Operational Mode: This service allows the operator to select the current operational
37   mode. The operator shall be permitted to command the CLE into the following modes:

38
39   a) Clear Mode
40   b) Standby Mode
41   c) Secure Mode
42   d) Clear Pending Secure Mode (Dial-Up only)
43   e) Standby Pending Secure Mode (Dial-up only)

44

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

08/31/98   ES-14885-4 Rev A

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.

7. Display Manufacturing Info: This service allows the operator to display the following information:

e) Firmware Revision

f) Firmware Date

g) Hardware List

h) Hardware Issue

i) Manufacturing Date

j) Unit Serial Number

k) Line Interface Unit (LIU) Type

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

m) SNMP Key Size, and Encryption Mode and Algorithm

8. Set Default Configuration

9. Firmware Update

4.3 Physical Security

1. Access to the circuitry contained within the CLE shall be restricted by the use of a Medeco lock. It shall not be possible to remove the enclosure cover without unlocking the lock.

2. The CLE shall include tamper response and zeroization circuitry. Upon the removal of the enclosure's cover, all plaintext cryptographic key and unprotected critical security parameters shall be immediately zeroized. This capability shall be operational whether or not power is applied to the module.

3. The CLE shall not employ ventilation holes, and shall be designed to prevent physical probing inside the enclosure.

4.4 Operating System Security

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 pervious 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.

9

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

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

12. If a successful 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 Manager 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 nor =t be displayed after user entry, and shall be zeroized by operator command or by a tamper situation.

4.6   Crypto Algorithms

1. The CLE shall use the Data Encryption Standard (DES) algorithm or Triple DES to protect the NRZ 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) General Purpose Memory Test

   d) Non-Volatile Memory Integrity Test

   e) Real Time Clock Test

   f) Cipher Chip Test

   g) Random Number Generator Test

   h) General Cryptographic Algorithm Test

   i) Pairwise Consistency Test

08/31/98   ES-14885-4 Rev A

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 and before the key is used or stored for later use.

   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

1   (24) Far End CLE Serial Number

2   (25) Far End CLE Serial Number timestamp

3   (26) Last Key Change Timestamp

4   (27) Event Log

5   (28) Key Change Method

6   (29) Begin Time

7   (30) End Time

8   (31) Days Interval

9   (32) Clear Modes

10   (33) Key Management Mode

11   (34) Manual Authentication Key

12   (35) Algorithm Adaptation Flag

13   (36) Exclusion List: For Dial-Up operation

1

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.

Security Relevant Data Items (PM=PrivaCy Manager, CLE=Cylink Link Encryptor) — **Role**

User/Crypto Officer Service	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
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