

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 A

July 24, 1998

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	User Role..... 4
9	4.2.2	Crypto Officer Role..... 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..... 11

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 Link Encryptor System shall be referred to as the CLE (Cylink Link
 22 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	2
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 Physical Security.

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
32
33
34
35

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. An operator that gains control of the CLE shall simultaneously assume both the User and Crypto Officer roles. Access to these roles are 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. Concurrent operator access/operation is prevented by disallowing SNMP access 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 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

1
2 **4.2.2 Crypto Officer Role**

3
4 The Crypto Officer Role provides the operator the ability to perform all of the services listed
5 below.

6
7 **1. Alarm/Event Services**

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

10 d) **Clear Event Log:** This service allows the operator to completely clear the contents of
11 the event log.

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

14 **3. Key Management**

15 a) **Set Auto Key Change Attributes**

16 b) **Days Interval**

17 c) **End to End Delay**

18 d) **Clear Modes Allowed/Disallowed**

19 e) **Mode Managed/Unmanaged**

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

22 (i) **CLE Network Certificate**

23 (ii) **CLE DSS secret key (X)**

24 (iii) **PrivaCy Manager DSS public key**

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

26 (v) **PrivaCy Manger/CLE SNMP message counter**

27 (vi) **CLE/CLE encryption key**

28 (vii) **Far End CLE serial number**

29 (viii) **Last key change timestamp**

30 (ix) **Event Log**

31 **4. Set Line Interface Configuration Parameters**

32 **5. Network Management**

33 a) **Display/Set Unit IP Address**

34 b) **Display/Set Gateway IP Address**

35 c) **Display/Set Subnet Mask Address**

1 d) Display/Set Trap1/Trap2 IP Address

2 6. System Test: This service allows the operator to set a Network Encryptor Loopback, or
3 a DTE Encryptor Loopback, or clear a loopback that has been previously set.

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

6 a) Firmware Revision

7 b) Firmware Date

8 c) Hardware List

9 d) Hardware Issue

10 e) Manufacturing Date

11 f) Unit Serial Number

12 g) Line Interface Unit (LIU) Type

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

14 i) SNMP Key Size, and Encryption Mode and Algorithm

15 8. Set Default Configuration

16 9. Perform Network Certification

18 4.3 Physical Security

19
20 1. Access to the circuitry contained within the CLE shall be restricted by the use of a
21 Medeco lock. It shall not be possible to remove the enclosure cover without unlocking
22 the lock.

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

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

31 4.4 Operating System Security

32
33 The FIPS 140-1 operating system requirements (FIPS PUB 140-1 section 4.7) do not apply to
34 the CLE because it is not a general purpose computer and thus it cannot run untrusted user-
35 supplied software. However, the CLE's firmware can be field updated using a download
36 process. The following rules apply to the downloading of new CLE firmware.

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

6 **4.5 Key Management**

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

20 If any of the tests fail the PrivaCy Manager/CLE encryption key and the newly loaded
21 Network Certificate are rejected and the CLE shall report the failure at the end of the
22 protocol.

- 23 6. A new CLE/CLE encryption key shall be negotiated each time the CLE transitions from
24 a non-secure state to a secure state.
- 25 7. While in the secure mode the CLE/CLE encryption key shall be periodically re-
26 negotiated.
- 27 8. CLE/CLE encryption keys shall be established using the Diffie-Hellman Key Agreement
28 process.
- 29 9. When establishing a new CLE/CLE encryption key, the messages containing the Diffie-
30 Hellman public component shall be signed.
- 31 10. Prior to accepting the CLE/CLE encryption key each CLE shall:
32 a) Verify the compatibility of the two units' session settings:
33 b) Verify the validity of the Network Certificate's signature.
34 If any of the above tests fail the CLE/CLE encryption key shall be rejected.

- 35
- 36 11. If the link encryption key generation process fails, the CLE shall generate an alarm.

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

4 **4.6 Crypto Algorithms**

- 6
- 7 1. The CLE shall use the Data Encryption Standard (DES) algorithm or Triple DES to
8 protect the NRZ line data. Sensitive PrivaCy Manager/CLE data shall be protected
9 using the Triple DES algorithm.
- 10 2. The CLE shall use the Digital Signature Standard as described in FIPS 186 for the
11 authentication of all security related information.
- 12 3. As specified in FIPS 186, the module will also support the Secure Hash Standard
13 (SHA-1) as described in FIPS 180-1.

14 **4.7 Self Test**

- 15
- 16
- 17 1. The following Power-Up Self Tests shall be performed when power is first applied to the
18 system.
- 19 a) Field Programmable Gate Array (FPGA) Test
- 20 b) Program Memory (ROM/FLASH) Integrity Test
- 21 c) General Purpose Memory Test
- 22 d) Non-Volatile Memory Integrity Test
- 23 e) Real Time Clock Test
- 24 f) Cipher Chip Test
- 25 g) Random Number Generator Test
- 26 h) General Cryptographic Algorithm Test
- 27 i) Pairwise Consistency Test
- 28
- 29 2. During normal operation, once during each second the battery that backs up the non-
30 volatile RAM shall be tested.
- 31 3. All keys to be used for symmetric key cryptographic algorithms shall be checked to
32 verify that they are cryptographically suitable for use as an encryption/decryption key.
33 This check shall be performed immediately after the value of the key has been
34 established and before the key is used or stored for later use.

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

3 **5 Definition of Security Relevant Data Items (SRDIs)**

- 4
- 5 (1) CLE Manufacturing Certificate
- 6 (2) PrivaCy Manager Manufacturing Certificate
- 7 (3) PrivaCy Manager/CLE SNMP Encryption Algorithm Flag
- 8 (4) PrivaCy Manager/CLE SNMP Encryption Mode Flag
- 9 (5) PrivaCy Manager/CLE SNMP Encryption Key Size Flag
- 10 (6) CLE to CLE Encryption Algorithm Flag
- 11 (7) CLE to CLE Encryption Mode Flag
- 12 (8) CLE to CLE Encryption Key Size Flag
- 13 (9) Near End Network Certificate
- 14 (10) Far End Network Certificate
- 15 (11) PRNG Running Seed (XKEY)
- 16 (12) CLE DSS Secret Key (X)
- 17 (13) CLE DSS Public Key (Y)
- 18 (14) PrivaCy Manager DSS Public Key
- 19 (15) PrivaCy Manager/CLE (SNMP) Encryption Key
- 20 (16) PM/CLE Message Counter Value
- 21 (17) PrivaCy Manager/CLE Message Counter
- 22 (18) CLE/CLE Encryption Key
- 23 (19) Near End CLE Challenge Value
- 24 (20) Far End CLE Challenge Value
- 25 (21) Voice Authentication Hash Value
- 26 (22) Far End CLE Serial Number
- 27 (23) Far End CLE Serial Number timestamp
- 28 (24) Last Key Change Timestamp
- 29 (25) Event Log
- 30 (26) Key Change Method
- 31 (27) Begin Time
- 32 (28) End Time

- 1 (29) Days Interval
- 2 (30) Clear Modes
- 3 (31) Mode

1

2 6 Definitions of SRDI Modes of Access

3

4

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:

5

6

7

a) **D** - The SRDI is set back to the manufacturing default by the service.

8

b) **G** - This service generates the SRDI internal to the CLE.

9

c) **I** - The SRDI is input into the CLE by this service.

10

d) **R** - The SRDI is read and used by the service.

11

e) **U** - The SRDI is updated by the service.

12

f) **V** - The SRDI is verified by the service.

13

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		
Perform Network Authentication	A	
Renewal of Network Authentication	M	
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 Mode Managed/Unmanaged		
Zeroize Keys		
Set Line Interface Parameters		
Set CLE IP Address		
Set Gateway IP Address		
Set Subnet Mask		
Set Trap1 IP Address		
Set Trap2 IP Address		
Display System Info		
Set/Clear DTE/NET Loopbacks		
Set Default Configuration		
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 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		

Table 1 Services Versus SRDI Access