CYLINK

Frame Encryptor Security Policy External Specification

ES-14976-0-02

Rev. G

December 5, 2001

1. Scope of Document

This document contains the security policy requirements for the Cylink Frame Encryptor system module and is applicable to all CFE-family devices including: CFE, CFE II and CFE HSSI. The Cylink Frame Encryptor System shall be referred to as the CFE in this document.

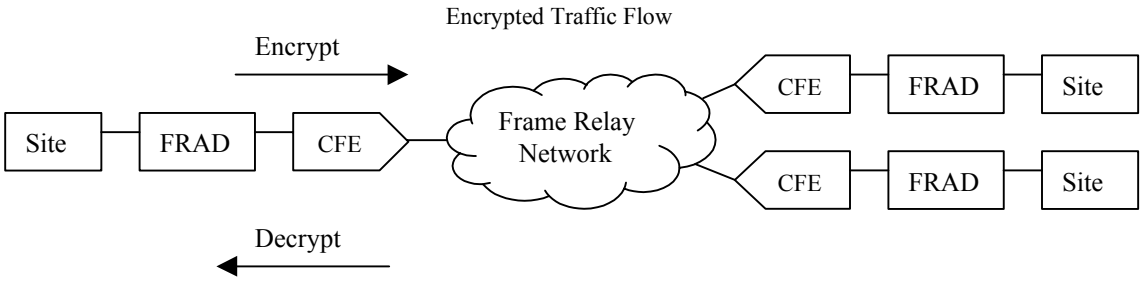
2. Applicable Documents

- 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. CFE Functional Overview

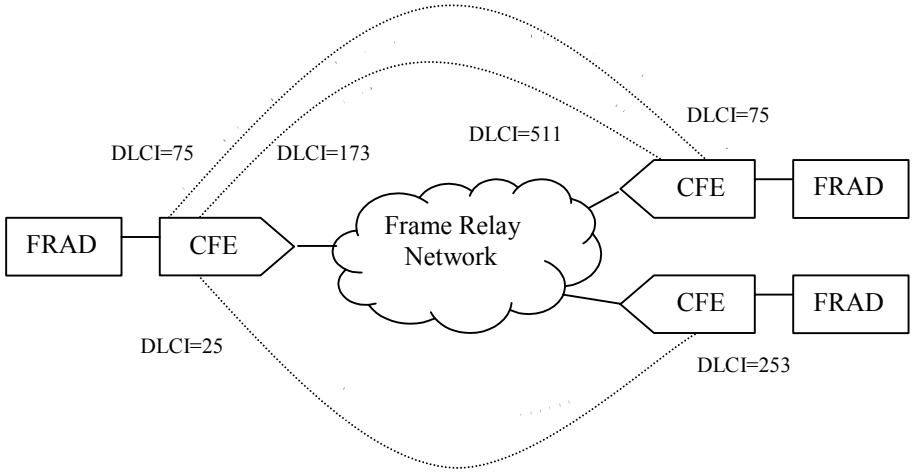
The CFE protects information flowing between nodes or sites of a frame relay network. The CFE can be configured to either allow or disallow information flow between two frame relay nodes. Furthermore, the information flow can be either protected through encryption or passed without encryption.

The role of the CFE is illustrated in the figure below. The CFE is installed between a FRAD (Frame Relay Access Device) and a Frame Relay Network. A CFE dynamically discovers other CFEs in the network and builds secured connections between itself and the CFEs. The CFEs selectively encrypt, reject, or pass in the clear frames flowing from the FRAD to the network. Conversely the CFEs selectively decrypt, reject, or pass information flowing from the network to the FRADs.



Secured connections are automatically established between the cryptographic module and similar units using a Diffie-Hellman key exchange process. This results in a separate secure link per connection and does not require any secret connection keys to ever be displayed or manually transported/installed. Secret connection keys will never leave the secure boundary in clear text form and they are not stored in non-volatile memory in clear text form.

The figure below shows an example of secured connections between secure units. Since a secured connection is based on the DLCI (Data Link Connection Identifier), it is possible to have more than one secured connection between two secure units. Since the frame relay network can change the value of the DLCIs, the DLCIs at each end of a secure connection usually have different values. In the example below there are 3 secured connections: 75&75, 173&511, and 25&253. A CFE can support a maximum of 1024 simultaneous secured connections. There are actually 976 connections available to the user at a frame relay network interface conforming to the Frame Relay Forum agreements; 48 more are reserved for user/net management.



4. Security Level

The CFE Cryptographic Module (CM) meets the overall requirements applicable to Level 3 security of FIPS 140-1.

Security Requirements Section	Level
Cryptographic Module	3
Module Interfaces	2/3
Roles and Services	2/3
Finite State Machine	3
Physical Security	3
EFP/EFT	N/A
Software Security	3

Operating System Security	N/A
Key Management	3
Cryptographic Algorithms	3
EMI/EMC	3
Self Test	3

5. Security Rules

This section documents the security rules enforced by the Cryptographic Module (CM). There are three levels of operation - Non-FIPS mode, FIPS Level 2, and FIPS Level 3.

The CM provides a FIPS mode enable/disable capability and requires the use of the Cylink PrivaCy Manager to enable and setup FIPS mode operation. To use the CM in FIPS 140-1 Level 2 or Level 3 mode, the unit must be configured to use TDES for user data encryption. In addition, the CM provides a Console interface (described below), which meets FIPS 140-1 Level 2 criteria when the Console User roles are entered. To use the CM in FIPS 140-1 Level 3 mode, the Console interface must not be used and the PrivaCy Manager must enable FIPS mode.

5.1 Cryptographic Module

As a result of a critical alarm condition (such as entry into the Tampered Mode) or a power failure, the CM shall not permit the automatic transmission of plain-text data over secured connections on Frame Relay interface.

5.2 *Module Interfaces*

The Crypto Officer accesses the module through either the Ethernet Data port, the Remote Serial port, the Clear Data port or the Cipher Data port. The Console User accesses the module through the Local Serial port.

The Clear Data/Cipher Data port is not used for un-protected transfer of key components, authentication data, or critical security parameters. All such traffic on this port is protected by digital signatures and/or is encrypted. This port is physically separate from all other ports in the CM.

5.3 *Roles and Services*

The CM shall support three User Roles, a Crypto Officer Role, and a Maintenance Role. The *Console Full User Role* is assumed to obtain various network configuration and module performance monitoring services. The *Console Read-Only User Role* is assumed to obtain various module performance monitoring services. The *Network User Role* is assumed to obtain data encryption and decryption services. The *Crypto Officer Role* is assumed to perform security management functions and fault and performance auditing. The *Maintenance Role* is

assumed to perform various functions to assist in the diagnosis and repair of the module.

When the CM is operating without the console attached, it is operating at FIPS 140-1 Level 3. Only the Crypto Officer role and the Network User role are available for this configuration. When the CM is operating with the console attached, it is operating at FIPS 140-1 Level 2. The Crypto Officer role, the Network User role, the Console Full User role, the Console Read-Only role, and the Maintenance role are available for this configuration. The console roles (Console Full User, Console Read-Only, and Maintenance) are provided for non-standard CM initialization/trouble-shooting and for system status reports. Security related functions such as Restore to Defaults and Tamper (performs zeroization) are available through the console.

The CM shall be designed in such a manner that no single point failure shall be capable of causing the module to pass plaintext data through the module on a secure connection. For the module to pass data in the clear, there are "two independent internal actions required." The policies, which allow plaintext data to be passed through the module, are established by two separate Crypto Officer configuration services and are implemented by two separate processes within the CM.

5.3.1 Crypto Officer Role

The Crypto Officer Role provides the operator the ability to:

Perform Network Certification	This service allows the operator to: • Load a Network Certificate into the Cryptographic Module • Establish a PrivaCy Manager / CM connection encryption key
Establish Console User Passwords	This service allows the operator to establish one or more console username and their associated passwords. Each username is configured to authorize the username to assume one or more console roles.
Set Operating Mode	This service allows the operator to select the current operational mode. The operator shall be permitted to command the Cryptographic Module into the following modes: • Offline • Operational • Locked
Show Status	Output the current status of the Cryptographic Module: • Active roles • Cryptographic state of module. • Cryptographic Module is in error state, error code • If bypass capability exists, whether the bypass capability is enabled (on all channels / connections).
Set Default Configuration	This service allows the operator to force parameters settings back to their pre-configured default values.
Set Cryptographic Parameters	This service allows the operator to: • Sets the Maximum Connection Rekey Time • Sets the Failed Connection Retry Interval • Sets the Connection Setup Timeout Interval
Define Security Policy Parameters	This service allows the operator to: • Set (optional) rule to block all traffic on a given

	connection • Set (optional) permission to bypass security measures for a connection • Set the CM Offline-Policy • Define Secure Group Policy • Define Secure Group Membership
Configure Trap Destination table	This service allows the operator to configure and display the CM's trap destination table.
Reset Unit	This service allows the operator to reset (power-cycle) the CM.
Download Software	This service allows the operator to download a new firmware image to the Cryptographic Module.
Set FIPS 140-1 Mode	This service allows the operator to select whether FIPS 140-1 mode is enabled or disabled.
Define Second Action Policies	This service allows the operator to specify the "second action" required when data is to be passed in the clear. There are a number of settings so that the operator can selectively allow the passing of data for different traffic types.

5.3.2 Network User Role

The Network User Role provides the operator with the ability to:

Encrypt data	Encrypts data arriving on the CM's clear port and transmits it out the CM's cipher port.
Decrypt data	Decrypts data arriving on the CM's cipher port and transmits it out the CM's clear port.
Block data	Blocks data arriving on both the CM's cipher and clear ports.
Pass data	Passes data arriving on both the CM's cipher and clear ports.

5.3.3 Console Full User Role

The Console Full User Role provides the operator the ability to:

Tamper	This service allows the operator to cause the unit to respond as though it had been physically tampered. This will result in: • An active zeroization of all secret keys. • A software reset upon the cryptographic module This will require the full tamper recovery process
Reset Unit	This service allows the user to reset (power-cycle) the CM.
Set Time	This service allows the operator to set the system clock.
Display Alarms	This service allows the operator to scroll through and view the contents of the CMs alarm queue.
Clear Alarm Condition	This service allows the operator to acknowledge an alarm condition. This will turn off the unit's Alarm LED.
Set Line Interface Parameters	This service allows the operator to configure the Line Interface. Items such as which clock source/type to use can be set.
Network Management	• Display/set Cryptographic Module IP Address: This service allows the operator to display or set the value of the current IP address to which the Cryptographic Module will respond.

	• Display/set connection (DLCI, etc.) to operate in loop back (for troubleshooting) • Disable loop-back on connection (DLCI, etc.)
Display System Information	This service allows the operator to display the following information: • Software Revision • Hardware List • Serial Number
Display Network Statistics	This service allows the operator to display network statistics for each port and connection.
Display Cryptographic Connections	This service allows the operator to display: • The state of each connection (DLCI, etc.) • Traffic statistics of each connection (DLCI, etc.)

5.3.4 Console Read-Only User Role

The Console Read-Only User Role provides the operator the ability to:

Display Alarms	This service allows the operator to scroll through and view the contents of the CMs alarm queue.
Network Management	• Display Cryptographic Module IP Address: This service allows the operator to display the current IP address to which the Cryptographic Module will respond. • Display connection (DLCI, etc.) to operate in loop back (for troubleshooting)
Display System Information	This service allows the operator to display the following information: • Software Revision • Hardware List • Serial Number
Display Network Statistics	This service allows the operator to display network statistics for each port and connection.
Display Cryptographic Connections	This service allows the operator to display: • The state of each connection (DLCI, etc.) • Traffic statistics of each connection (DLCI, etc.)

5.3.5 Maintenance Role

The Maintenance Role is only assumed after appropriate authentication and after all plaintext secret and private keys and other critical security parameters have been cleared (this is done by internally tampering the CM). The Maintenance Role provides the operator with all services provided by the Console User roles and additionally the ability to:

Zeroize System Memories	This service allows the operator to clear the various system memories thereby zeroing current configuration setting and certificates.
Set Default Configuration	This service allows the operator to force all settings back to the manufacturing default values.
Invoke Self Tests	This service allows the operator to perform the following module tests: • SRDI (Security Relevant Data Items)

		and configuration data (Battery backed SRAM) integrity test. • Encryption Engine Test • Exponentiation Engine Test • Random Number Generator Test • General Cryptographic Algorithm Test • System Loopback Encryption Test

5.3.6 Operator Authentication

The CM performs identity-based authentication of the operator accessing the module to determine that the operator is authorized to assume a specific role (and to perform its associated services). Two mechanisms are employed to provide authentication - Cylink Digital Certificates using public key technology and passwords.

Passwords are used to authenticate an operator (username) on the dedicated Local Serial interface to the Console Full User Role, the Console Read-Only User Role, or the Maintenance Role. An operator authenticated to the Crypto Officer role establishes the username, password, and role associations used by the CM.

Identity and authentication of an operator (PrivaCy Manager) to the Crypto Officer Role is based upon a public key certificates and the secure SNMP encryption key that is generated during a certificate loading process.

Identity and authentication of an operator (another CM) to the Network User Role is based upon an exchange of public key certificates and the encryption key that is generated during a certificate exchange process. In this case, a CM initiates a request for service when network traffic on a particular network channel (DLCI, etc.) is received. However, a CM will not authenticate another CM for the Network User Role until the Crypto Officer has configured the module by issuing a Protected Entity Certificate which defines the module's secure group and encryption algorithm configuration. This certificate contains the module's public number and is signed with the PrivaCy Manager private DSS number.

5.3.7 Tamper Recovery

The CM performs automatic zeroization of all authentication data if the module is opened while the unit is powered-on or powered-off. See the Physical Security section below. This zeroization (tampering) will require re-authentication of Network User role and Crypto Officer roles before services can be obtained using these roles. This process requires a trusted operator using the module's console interface and a trusted operator using the PrivaCy Manager interface.

5.4 Physical Security

1. All active devices shall employ standard commercial grade passivation techniques.
2. The CM shall be entirely contained within a commercial grade enclosure that shall be opaque within the visible spectrum.
3. The CM shall include tamper response and zeroization circuitry. The service access 'door' (being closed) of the 'strong' enclosure shall cause a Momentary On Micro Switch to be held

depressed (inactive). When the door is opened the switch shall cause a tamper signal to be sent which as a result shall actively zeroize (erase) the internal encryption keys that would allow the SRDIs stored in battery backed SRAM to be decoded. This capability shall be operational whether or not external power is applied to the module.In addition, when 'tampered', the power to the battery backed SRAM shall be removed. This capability shall be operational whether or not external power is applied to the module.If the Cryptographic Module has power when the tamper signal is active, the Software shall cause ALL secure information in volatile memory locations to be actively zeroized.

4. If the CM employs ventilation holes, they shall be small and constructed using 90-degree blocking barriers in a manner that prevents physical probing inside the enclosure.
5. In addition, opening the service access 'door' of the Cryptographic Module shall be passively detected by tamper evident "Holographic" seals on the outside of the 'door'.

5.5 *Key Management*

1. The CM shall employ the Pseudo Random Number Generator (PRNG) defined in FIPS 186 Appendix 3.1 using the (SHA-1) G(x) function defined in FIPS 186 Appendix 3.3.
2. The PRNG seed (referred to as the XKEY in FIPS 186 Appendix 3.1) shall be installed into the CM using the Cylink Manufacturing Configurator (CMC).
3. During the installation process of the CM Network Certificate, a PrivaCy Manager/CM encryption key shall be established.
4. PrivaCy Manager/CM encryption keys shall be re-negotiated each time a new CM Network Certificate is loaded.
5. PrivaCy Manager/CM encryption keys shall be stored in the module in encrypted form using a master key stored in automatically erasable memory (when the module is tampered).
6. PrivaCy Manager/CM encryption keys shall be established using the Diffie-Hellman Key Agreement process.
7. Messages exchanged between the PrivaCy Manager and the CM systems that contain the Diffie-Hellman public components used to establish the PrivaCy Manager/CM encryption key shall be signed using the DSA associated with each entities Manufacturing Certificate.
8. Prior to accepting the PrivaCy Manager/CM DH public number/component, the CM shall perform the following verifications:

   Using the public key of the Cylink Certificate Authority (CCA), verify the signature of the PrivaCy Manager Manufacturing Certificate.

   Verify the value of the challenge bits in the message received from the PrivaCy Manager system.

   Verify the signature of the message conveying the Network Certificate and the Diffie-Hellman public component from the PrivaCy Manager using the PrivaCy Manager public DSS key from the PrivaCy Manager Manufacturing Certificate.
9. If any of the above tests fail, the PrivaCy Manager/CM DH public number and the newly loaded Network Certificate are rejected and the CM shall report the failure at the end of the protocol exchange.
10. A new CM/CM encryption key shall be negotiated each time the CM receives a connection setup request.

11. The CM/CM encryption key shall be periodically re-negotiated as configured by the PrivaCy Manager.
12. The CM/CM encryption key shall be stored in the module in encrypted form using a master key stored in automatically erasable memory (when the module is tampered).
13. CM/CM encryption keys shall be established using the Diffie-Hellman Key Agreement process.
14. When establishing a new CM/CM encryption key, the messages containing the Diffie-Hellman public component shall be signed using the CM's DSS Signature Key found in each CM's Protected Entity Certificate.
15. Prior to accepting the CM/CM encryption key each CM shall perform the following verifications:

    Verify the compatibility of each of the following from the session settings:

    - Protocol Type.
    - Algorithm and Encryption Mode.
    - Length of Diffie-Hellman public component.
    - Challenge Value.

    Verify the validity of the Protected Entity Certificate's signature using the DSS Public key of the managing PrivaCy Manager system.

    Verify the compatibility of each of the following from the far end Protected Entity Certificate:

    - Certificate Type.
    - Product Type.
    - Customer ID.
16. If any of the above tests fail the CM/CM encryption key shall be rejected.

5.6 *Cryptographic Algorithms*

The following algorithms are supported:

1. Triple DES CFB8 (ANSI X9.52)
2. Triple DES CFB64
3. DES CFB8 (FIPS 46-2)
4. DES CFB64
5. Digital Signature Standard (FIPS 186)
6. Secure Hash Standard (FIPS 180-1)

5.7 *EMI/EMC*

- The Cryptographic Module shall meet the requirements specified in FCC Part 15 subpart J, Class B.
- The module shall in addition meet the European market requirements regarding Electro-Magnetic Radiation and Susceptibility as necessary to obtain the EC stamp.

5.8 *Self Test*

1. The following Power-Up Self-Tests shall be performed when power is first applied to the system:
   a) Program Memory (ROM/FLASH) Integrity Test: This test consists of verifying the integrity of the selected Program Memory by computing an error detection code value over the firmware image and comparing it with the expected value stored in the image.
   b) General Purpose Memory Test: This test verifies that all volatile system memory address and data buses can be written to and read from.
   c) Non-Volatile Memory Integrity Test: This test consists of verifying the integrity of the data stored in both the EEPROM and the battery-backed RAM. CRC values are calculated for each the stored data item and then compared to stored expected values.
   d) Real Time Clock Test: This test consists of verifying that the data returned by the real time clock is a valid data and time.
   e) Cipher Chip Test: This test verifies that the cipher chip is functioning properly. This is done by performing a Known Answer Test (KAT) for both the encrypt and decrypt functions for each value of feedback supported.
   f) Exponentiation Chip Test: This test verifies that the exponentiation chip is functioning properly. Known Answer Tests (KAT) are performed for all functions provided by the chip.
   g) Random Number Generator Test: This test verifies the proper operation of the Random Number Generator using the FIPS 140-1 Continuous Random Number Generator Test specified in FIPS 140-1 section 4.11.2 paragraph 5.
   h) General Cryptographic Algorithm Test: This test verifies the proper operation of the other cryptographic operations of the module. This includes SHA-1 (corresponding to FIPS PUB 182), and DSA (corresponding to FIPS PUB 186).
2. The following Maintenance Role Invoked Self-Tests shall be provided:
   a) Cipher Chip Test: This test verifies that the cipher chip is functioning properly. The encrypt and decrypt functions for each value of feedback supported are tested using fixed data patterns and key patterns and verifying the results using a FIPS certified software standard.
   b) Exponentiation Chip Test: This test verifies that the exponentiation chip is functioning properly. Each of the functions provided by the chip is tested with random data patterns and verified using a FIPS certified software standard.
   c) Random Number Generator Test: This test verifies the proper operation of the Random Number Generator using the FIPS 140-1 Continuous Random Number Generator Test specified in FIPS 140-1 section 4.11.2 paragraph 5.
   d) General Cryptographic Algorithm Test: This test verifies the proper operation of the other cryptographic operations of the module. This includes SHA-1 (corresponding to FIPS PUB 182), and DSA (corresponding to FIPS PUB 186).
   e) System Loopback Encrypt/Decrypt Test: This test verifies the proper operation of the clear and cipher data ports in conjunction with the Cipher Chip. Fixed data patterns are transmitted on the cipher data port and ‘looped-back’ (internally or using a cable) to the clear data port, where they are encrypted (using fixed key patterns) with each supported encryption method. The result verified using a FIPS approved software standard. The result is then transmitted on the clear data port and ‘looped-back’ (internally or using a cable) to the cipher data port, where they are decrypted and verified (as matching the original data pattern).

3. During normal operation, each time data is requested from the Random Number Generator, the Continuous Random Number Generator Test specified in FIPS 140-1 section 4.11.2 paragraph 5 shall be performed.
4. During normal operation, each time a Digital Signature is generated, the Pairwise Consistency Test is performed as specified in FIPS PUB 140-1 section 4.11.2 pp.34. This test verifies the digital signature on each message being signed.
5. 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.

6. Definition of Security Relevant Data Items (SRDIs)

SRDI	Description
CM Manufacturing Certificate	This is the certificate that is produced and signed by the Cylink Certification Authority that identifies the cryptographic module.
CM Network Certificate	This is the certificate that is produced and signed by the managing PrivaCy Manager system
CM Protected Entity Certificate (PEC)	This is the certificate that is produced and signed by the managing PrivaCy Manager system. It is used to negotiate connections with remote modules.
CM DSS Signature Secret Key (X)	This is the secret component of the Cryptographic Module DSS Signature Key.
CM DSS Signature Public Key (Y)	This is the public component of the Cryptographic Module DSS Signature Key.
PM Manufacturing Certificate	This is the certificate that is produced and signed by the Cylink Certification Authority that identifies the managing PrivaCy Manager system.
PM DSS Signature Public Key	This is the public component of the PrivaCy Manager DSS Signature Key.
CM / PM Encryption Key	This is the encryption / decryption key used by the Cryptographic Module and the managing PrivaCy Manager system.
CM / PM Command Counter	This is a counter used to prevent replay attacks on the management network used to control the Cryptographic Module.
Permitted Crypto Methods	This specifies the set of crypto methods that may be used to build a connection with a remote module.
Rekey Parameters	CM - CM rekey parameters
CM - CM Keys	These are the encryption / decryption keys used to secure the communications between two Cryptographic Modules.
Connection configuration	Specifies the policy for each connection
Insecure Communicatio n Policy	Specifies special traffic handling policies for Offline, Tamper, NRU, etc.
Group Policy	Specifies the traffic handling policy to be used by secure groups
Trap Destination Table	Lists the nodes to be sent traps.
System Time	Real time clock
FIPS Configuration	Specifies FIPS 2nd Action traffic handling policies and FIPS mode setting.
Username-Password Table	Username, password, and role associations for operator logging on console.

7. 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.
b) **G** - The SRDI is generated.
c) **R** - The SRDI is read.
d) **U** - The SRDI is read then updated.
e) **S** - The SRDI is set.
f) **Z** - The SRDI is erased by the service.
g) **L** - The SRDI is loaded by the service.

When the CM is operating without the console attached, it is operating at FIPS 140-1 Level 3. Only the Crypto Officer role and the Network User role are available for this configuration. The following two pages describing SRDI Modes of Access address the Crypto Officer role and the Network User role. Refer to the Roles and Services section above for details concerning the services for these roles.

When the CM is operating with the console attached, it is operating at FIPS 140-1 Level 2. The Crypto Officer role, the Network User role, the Console Full User role, the Console Read-Only role, and the Maintenance role are available for this configuration. The following four pages describing SRDI Modes of Access address these roles. Refer to the Roles and Services section above for details concerning the services for these roles.

Security Related Data Item vs Service	CM Manufact. Cert.	CM Network Cert.	CM Prot. Entity Cert.	CM DSS Secret Key	CM DSS Public Key	PM Manufact. Cert.	PM DSS Public Key	CM/PM Encryption Key	CM/PM Command Counter	Crypto Methods	Rekey Parameters	CM/CM keys	Connection Config.	Insecure Comm. Policy	Group Policy	Trap Destination Table	System Time	FIPS Configuration	Username/Password Table	
Perform Network Certif.																				
initial cert. issued	R	L		R,G	R,G	R	L	G	S	R										
same cert. rev. issued	R	R		R	R		R	R,G	S	R										
new cert. rev. issued	R	R,L		R, G	R,G		L	R,G	S	R										
Set Operating Mode								R	U	R										
Show Status									U		R		R	R	R		R	R	R	
Set Default Config.								R	U		D		D	D						
Set Crypto Parameters								R	U											
Set Sec. Policy Params			L					R	U	R			S	S	S					
Config. Trap Dest. Table								R	U	R						R,S				
Reset Unit								R	U							R				
Download Software							R	R	U											
Set FIPS Mode								R	U									S		
Set 2nd Action Policies								R	U									S		

Security Related Data Item vs Service	CM Manufact. Cert.	CM Network Cert.	CM Prot. Entity Cert.	CM DSS Secret Key	CM DSS Public Key	PM Manufact. Cert.	PM DSS Public Key	CM/PM Encryption Key	CM/PM Command Counter	Crypto Methods	Rekey Parameters	CM/CM keys	Connection Config.	Insecure Comm. Policy	Group Policy	Trap Destination Table	System Time	FIPS Configuration	Username/Password Table	
Encrypt Data										R	R	R,G	R		R			R		
Decrypt data										R	R	R,G	R		R			R		
Block Data											R		R		R			R		
Pass Data											R		R	R	R			R		

Security Related Data Item vs Service	CM Manufact. Cert.	CM Network Cert.	CM Prot. Entity Cert.	CM DSS Secret Key	CM DSS Public Key	PM Manufact. Cert.	PM DSS Public Key	CM/PM Encryption Key	CM/PM Command Counter	Crypto Methods	Rekey Parameters	CM/CM keys	Connection Config.	Insecure Comm. Policy	Group Policy	Trap Destination Table	System Time	FIPS Configuration	Username/Password Table	
Tamper		Z	Z	Z	Z		R,Z	R,Z	Z			Z			Z				Z,D	
Reset Unit																				
Set Time																	S			
Display Alarms																				
Clear Alarms																				
Set Interface Params																				
Network Management																				
Display System Info																	R			
Display Network Status																				
Display Crypto Conns													R							

Security Related Data Item vs Service	CM Manufact. Cert.	CM Network Cert.	CM Prot. Entity Cert.	CM DSS Secret Key	CM DSS Public Key	PM Manufact. Cert.	PM DSS Public Key	CM/PM Encryption Key	CM/PM Command Counter	Crypto Methods	Rekey Parameters	CM/CM keys	Connection Config.	Insecure Comm. Policy	Group Policy	Trap Destination Table	System Time	FIPS Configuration	Username/Password Table	
Zeroize System Memory	Z	Z	Z	Z	Z		Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	
Set Default Configuration		Z	Z	Z	Z		Z	Z	Z		D	Z	D	D	D	D	D	D	D	
Invoke Self Tests														R				R		