CM180D

Security Policy

Version 1.0

CipherMax, Inc.

December 5, 2008

TABLE OF CONTENTS

1. Module Overview

The CM180D (HW P/N 81-00038-01 Version ILC 6.11, FW Version 5.4.0.36) is a multi-chip standalone cryptographic module system that provides a network-based security solution for high performance tape encryption combined with SAN access control and Fibre-Channel switching in a compact, 1U form factor.

The cryptographic boundary of the module is defined as the outer perimeter of the metallic enclosure with all Field Replaceable Units (FRUs) removed. These Field Replaceable Units include three fans and two power supplies.

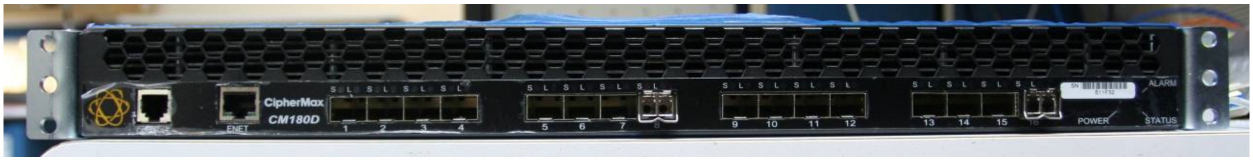


Figure 1 – CM180D Cryptographic Module

2. Security Level

The cryptographic module meets the overall requirements applicable to Level 2 security of FIPS 140-2.

Table 1 - Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	3
Module Ports and Interfaces	2
Roles, Services and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A

3. Modes of Operation

The module only supports an Approved mode of operation and supports the following FIPS Approved algorithms:

- AES (Certificate No. 629)
- TDES (Certificate No. 590)
- DRNG (Certificate No. 360)
- RSA Sign/Verify (Certificate No. 289)
- DSA Sign/Verify Certificate No. 241)
- SHA-1 (Certificate No. 670)
- HMAC SHA-1 (Certificate No. 326)

The module supports the following non-Approved algorithms:

- NDRNG
- MD5 to support TLS operations
- RSA Key Transport (key wrapping; key establishment methodology provides 80 bits of encryption strength)
- Diffie-Hellman within TLS and SSHv2 (key wrapping; key establishment methodology provides 80 bits of encryption strength)

4. Ports and Interfaces

The module supports the physical ports described below:

• Fiber Channel (Qty. 16):	Data Input/Output, Control Input, Status Output
• RJ-45 10/100 Ethernet:	Data Input/Output, Control Input, Status Output
• RJ-11 Serial Console:	Data Input/Output, Control Input, Status Output
• LEDs:	Status Output
• Power Ports:	Power Input

5. Identification and Authentication Policy

Assumption of roles

The cryptographic module shall support three distinct operator roles and three distinct system operator roles. The three operator roles authenticate by means of a username and password combination, where as the system roles authenticate by means of digital signature verification. Operator sessions are cleared when power is removed from the module and no feedback is provided to the operator during authentication that would weaken the strength of the authentication mechanism.

Table 2 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
Storage Admin	Identity-based operator authentication	Eight to 32 character password
User	Identity-based operator authentication	Eight to 32 character password
Security Admin (Cryptographic Officer)	Identity-based operator authentication	Eight to 32 character password
Cluster Device	Role-based operator authentication	Digital signature verification
SANCruiser MGMT Server	Role-based operator authentication	Digital signature verification
KeyCruiser	Role-based operator authentication	Digital signature verification

Table 3 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Username and Password	The probability that a random attempt will succeed or a false acceptance will occur is $1/96^8$ which is less than 1/1,000,000. The module will have a 30 second delay after every three consecutive authentication failures. The probability of successfully authenticating to the module within one minute is $6/96^8$ which

	is less than 1/100,000.
Digital signature verification	The probability that a random attempt will succeed or a false acceptance will occur is $1/2^{80}$ which is less than 1/1,000,000. The module will have a 30 second delay after every three consecutive authentication failures. The probability of successfully authenticating to the module within one minute is. $6/2^{80}$ which is less than 1/100,000.

6. Access Control Policy

Roles and Services

Table 4 – Services Authorized for Roles

Role	Authorized Services
Storage Admin	• Authorize Backup: Backup system and storage configuration. This backup does not contain any security related information. • View/Modify Storage Config • View Security Config • Create/View/Destroy Storage Admin or Users • Firmware Upgrade • Retrieve System Logs • Password Update
User	• View Storage Config • View Security Config • Password Update
Security Admin	• Authorize Backup: Backup security configuration information, including all keys and policies, to an external security database. Backup information is encrypted using TLS. • View Storage Config • View/Modify Security Config

	• Create/View/Destroy Security Admin • Retrieve Security Audit Logs • Zeroize: Actively overwrite all plaintext CSPs within the module. • Commission Existing Domain: Configure a module to join an existing security domain. • System Restoration: Restore the security database to a previous configuration or in its entirety from a backup. • Import Policy: Import Data Encryption Keys from another CM from a different domain. • Export Policy: Export DEK to an sFTP server for another CM • Password Update
Cluster Device	• Synchronize Configuration: Synchronize the configuration of two peer CMs.
SANCruiser MGMT Server	• View/Modify Storage Config • View Security Config • Firmware Upgrade • Retrieve System Logs • View Storage Config • View/Modify Security Config • Retrieve Security Audit Logs • System Restoration: Restore the security database to a previous configuration or in its entirety from a backup
KeyCruiser	• Authorize Backup: Backup the security database, which includes all CSPs and policies.

Unauthenticated Services

The module does not require an operator to assume an authorized role when performing the following services:

- Show Status
- Self-Tests
- SNMPv2

Definition of Critical Security Parameters (CSPs)

The following are CSPs contained in the module:

1. Recovery Key: Used to protect the Master Key
2. Master Key: Used to protect the Data Encryption Keys
3. Data Encryption Key: Used to protect data traffic
4. CipherMax Private Key: Used to authenticate to peer devices during TLS
5. CipherMax DSA Audit Log Private Key: Used to sign audit logs and also to authenticate sFTP servers
6. TLS Session Key: Used to secure communications with TLS peers
7. TLS Integrity Key: Used to provide data authentication for communications with TLS peers
8. RNG Seed and Seed Key: Used during the ANSI X9.31 generation of pseudo random numbers.
9. DH Private Key: Used to establish session keys
10. SSH Session Key: Used to secure communications with SSH clients
11. SSH Integrity Key: Used to provide data integrity for communications with SSH clients
12. SSH DSA Private Key: Used to authentication communications with SSH clients
13. sFTP Session Key: Used to secure communications with sFTP server
14. Passwords: Used to authenticate the Storage Admin, Security Admin, and User accounts

Definition of Public Keys

The following are the public keys contained in the module:

1. CipherMax Public Key (TLS): Used by peers during the TLS handshake
2. Cluster Device Public Key (TLS): Used by the CM to authenticate peer devices
3. DH Public Key: Used to establish session keys
4. SSH DSA Public Key: Used by SSH clients to authenticate the CM
5. CipherMax DSA Audit Log Public Key: Used by external entities to authenticate the cryptographic module
6. Certificate Authority Public Key: Used to verify the chain of trust for received public keys
7. CipherMax FW Verification Key: Used to verify FW images loaded into the cryptographic module
8. SANCruiser Public Key: Used to authenticate the SANCruiser
9. KeyCruiser Public Key: Used to authenticate the KeyCruiser

Definition of CSPs Modes of Access

Table 5 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as follows:

- Read
- Write
- Zeroize

Table 5 – CSP Access Rights within Services

Service	Cryptographic Keys and CSPs Access Operation
Authorize Backup	Read Master Key, Data Encryption Key Read TLS Session Key, TLS Integrity Key, CipherMax Private Key Read sFTP Session Key, CipherMax Audit Log Private Key
View/Modify Storage Config	Read SSH Session Key, SSH Integrity Key, SSH Private Key Read TLS Session Key, TLS Integrity Key, CipherMax Private Key
View Security Config	Read SSH Session Key, SSH Integrity Key, SSH Private Key Read TLS Session Key, TLS Integrity Key, CipherMax Private Key
Modify Security Config	Read SSH Session Key, SSH Integrity Key, SSH Private Key Read TLS Session Key, TLS Integrity Key, CipherMax Private Key Read sFTP Session Key, CipherMax Audit Log Private Key Read/Write Recovery Key, Master Key, Data Encryption Key, RNG Seed Key
Create/View/Destroy Storage Admin or Users	Read SSH Session Key, SSH Integrity Key, SSH Private Key Write Password (digest)
Firmware Upgrade	Read sFTP Session Key, CipherMax Audit Log Private Key

Retrieve System Logs	N/A
Password Update	Read SSH Session Key, SSH Integrity Key, SSH Private Key Write Password (digest)
Create/View/Destroy Security Admin	Read SSH Session Key, SSH Integrity Key, SSH Private Key Write Password (digest) Zeroize Password
Retrieve Security Audit Logs	N/A
Zeroize	Zeroize All Plaintext CSPs
Commission Existing Domain	Read SSH Session Key, SSH Integrity Key, SSH Private Key Read sFTP Session Key, CipherMax Audit Log Private Key Write Master Key, Recovery Key
System Restoration	Read SSH Session Key, SSH Integrity Key, SSH Private Key Read TLS Session Key, TLS Integrity Key, CipherMax Private Key Read sFTP Session Key, CipherMax Audit Log Private Key Write Master Key, Recovery Key, Data Encryption Keys
Import Policy	Read SSH Session Key, SSH Integrity Key, SSH Private Key Read TLS Session Key, TLS Integrity Key, CipherMax Private Key Read sFTP Session Key, CipherMax Audit Log Private Key Read Recovery Key, Master Key Read/Write Data Encryption Key
Export Policy	Read SSH Session Key, SSH Integrity Key, SSH Private Key Read TLS Session Key, TLS Integrity Key, CipherMax Private Key Read sFTP Session Key, CipherMax Audit Log

	Private Key Read DEK, Master Key
Synchronize Configuration	Read TLS Session Key, TLS Integrity Key, CipherMax Private Key Read/Write Master Key, Recovery Key, Data Encryption Keys

7. Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the module supports a limited operational environment and only allows the loading of trusted, validated code signed by CipherMax's FW Private Key.

8. Security Rules

The cryptographic module's design corresponds to the cryptographic module's security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 2 module.

1. When the module has not been placed in a valid role, the operator shall not have access to any cryptographic services.
2. The cryptographic module shall perform the following tests:

   Power On Self-Tests:

   - SHA-1 KAT
   - RSA Encrypt/Decrypt KAT
   - RSA Sign/Verify KAT
   - DSA Sign/Verify Pairwise Consistency Test
   - TDES Encrypt/Decrypt KAT (TDES only used for DRNG and TLS)
   - DRNG KAT
   - HMAC SHA-1 KAT
   - AES KAT
   - Firmware Integrity Check (32-bit EDC)

Conditional Tests

- NDRNG Continuous Test (64-bit blocks)
- DRNG Continuous Test (64-bit blocks)
- RSA Pairwise Consistency Test
- DSA Pairwise Consistency Test
- Firmware Load Test (DSA Signature Verification)
- Alternating Bypass Test

3. At any time the cryptographic module is in an idle state, the operator shall be capable of commanding the module to perform the power up self-test.
4. Data output shall be inhibited during key generation, self-tests, zeroization, and error states.
5. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
6. The module supports an alternating bypass capability. A Security Admin can configure the bypass capability at anytime using the "View/Modify Security Config" service. A change to the current configuration results in the execution of the Alternating Bypass Test.

9. Physical Security

The cryptographic module provides the following physical security mechanisms in order to comply with FIPS 140-2 Level 2 requirements:

- Commercial grade, production quality components
- Opaque enclosure
- Tamper-evident seals – One tamper-evident seal is placed over a screw, as shown in the picture below. The placement prevents the removal of the screw, which, in turn, prevents the removal of the cover. The tamper-evident seal is applied during manufacturing, and is the only tamper-evident seal applied to the module. There is only one removal cover, which is protected by this tamper evident seal.

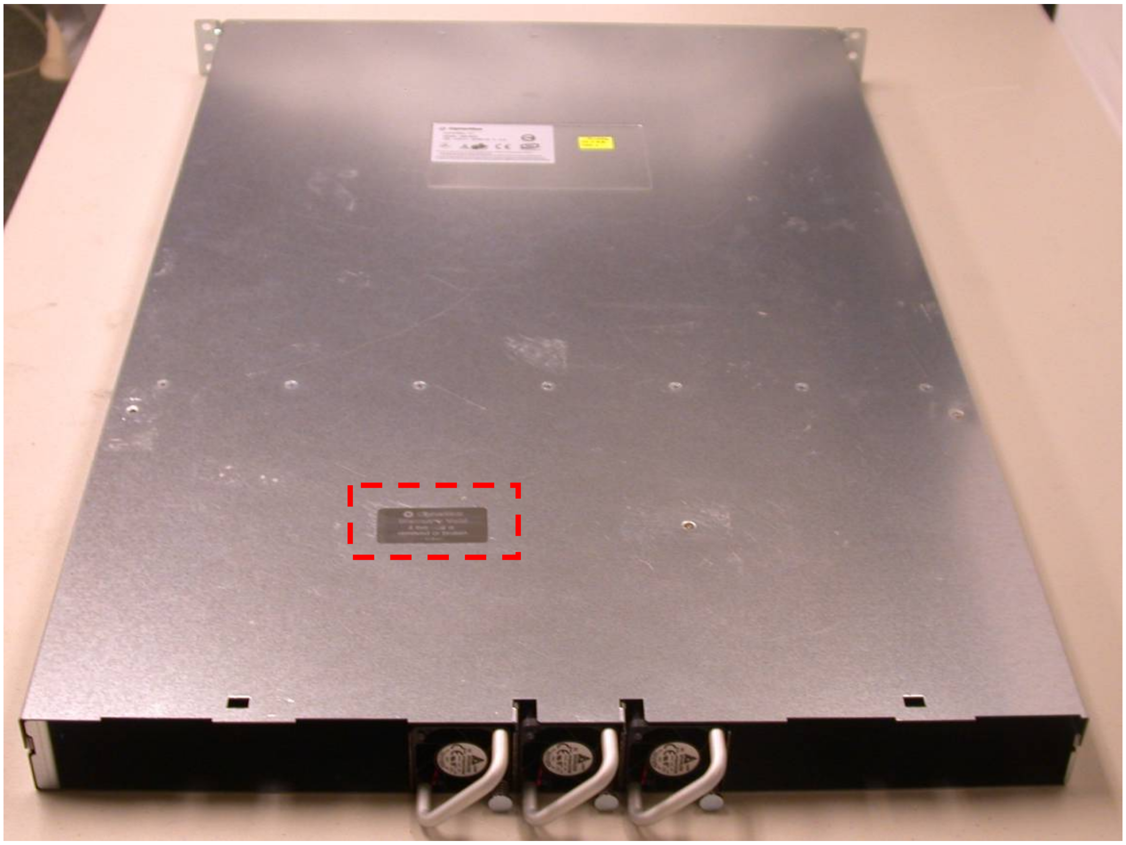
- 

Figure 2 – CM180D Tamper-Evident Seal Placement (shown in the red rectangle above)

10. Mitigation of Other Attacks Policy

The module has not been designed to mitigate any specific attacks.

11. Definitions and Acronyms

AES	Advanced Encryption Standard
DEK	Data Encryption Key
DRNG	Deterministic Random Number Generator
DSA	Digital Signature Algorithm
FRU	Field Replaceable Unit
LED	Light Emitting Diode
NDRNG	Non-Deterministic Random Number Generator
RNG	Random Number Generator
RSA	Rivest Shamir Adelman
sFTP	SSH File Transfer Protocol
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SSH	Secure Shell
TDES	Triple-Data Encryption Standard
TLS	Transport Layer Security