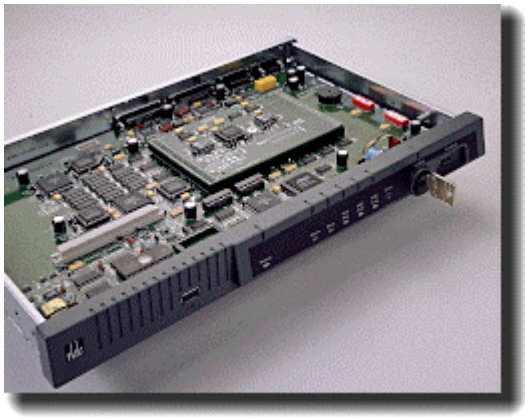
Technical Communications Corporation

CipherX® 7200



FIPS 140-1 Non-Proprietary Security Policy

Level 3 Validation

March 2000

Table of Contents

INTRODUCTION

1.1 Purpose

This is a Federal Information Processing Standards Publication 140-1 (FIPS 140-1) Security Policy for the Technical Communications Corporation's (TCC's) CipherX® 7200 Internet Protocol (IP) network encryptor. This Security Policy was produced as part of the level 3 certification of the CipherX® 7200 as required by FIPS 140-1. The Security Policy explains how the CipherX® 7200 meets all FIPS 140-1 level 3 requirements and details the secure operation of the CipherX® 7200.

1.2 References

This document discusses the security critical aspects of the CipherX® 7200 using FIPS 140-1 terminology and language. For more information on the CipherX® 7200, and the CipherX® Series of products please visit the TCC web site (http://www.tccsecure.com/).

This document is part of a complete FIPS 140-1 Certification Submission Documentation package that includes a proprietary Finite State Machine and proprietary Vendor Evidence document. For more information about the FIPS 140-1 standard and validation program visit the NIST website (http://csrc.nist.gov/cryptval/).

1.3 Document Organization

The Security Policy document is one document in complete FIPS 140-1 Submission Package. In addition to this document, the complete Submission Package contains:

- Vendor Evidence document
- Finite State Machine
- Module Software Listing
- Other supporting documentation as additional references

This Section serves as an introduction to the Security Policy, and is followed by a brief introduction to the CipherX® Series in section 1.4. Section 2 then discusses how the CipherX® 7200 addresses all of the FIPS 140-1 requirements. Section 3 describes the Self-Tests that the TCC module provides. Section 4 highlights the necessary configurations for FIPS-mode of operation. Throughout this document, the CipherX® 7200 may be referred to as the CipherX® 7200, CipherX®, or simply as the module.

This Security Policy and other Certification Submission Documentation was produced by Corsec Security, Inc. under contract to TCC. With the exception of this Non-Proprietary Security Policy, the FIPS 140-1 Certification Submission Documentation is TCC-proprietary and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact TCC.

1.4 The CipherX® Series

The CipherX® Series is a family of hardware-based data security systems that provide leading edge encryption for mission-critical wide area networks. The CipherX modules act as a network overlay, no network modification is required. The similarity across the CipherX family

minimizes operator training. All CipherX products are easily and centrally managed by TCC's KEYNET™ key and network management system, and support American National Standards Institute (ANSI) X9.19 fully automated key management. The automated architecture ensures ease of use, minimizes user action and maintains constant and reliable network security. The CipherX uses ANSI X9.52, two-key Triple DES for encrypting data and the SHA-1 algorithm for hashing.

2 The CipherX® 7200

The CipherX® 7200 IP Encryptor provides encryption for enterprise-wide networks. Its flexible design allows you to encrypt specific traffic flows, or to create a complete corporate Virtual Private Network that transparently secures all employee data. Security at the virtually ubiquitous IP layer allows the CipherX® 7200 to secure almost any Local Area Network (LAN), Wide Area Network (WAN), or hybrid network. To insure network performance, the CipherX 7200 provides IP encryption at data rates up to 10 Mbps. These services are provided in a single box that meets FIPS 140-1 Level 3 requirements.

2.1 High-Security, Low Profile

Through the use of custom-designed boards built for reliability and performance, the CipherX 7200 offers a very slim, rack-mountable profile. The CipherX 7200 is a multi-chip standalone cryptographic module, with the outer case defining the cryptographic boundary.

Figure 1 – Steel Covered Security in a Slim, Rack-Mountable Case

This solid steel cover completely encloses the CipherX 7200 to protect it from tampering, even through the baffled air vents, or sealed screw receptacles. A matte grey paint and plastic front bezel show signs of forced entry to the module, and any attempt to remove the top cover will trigger an active tamper response. The CipherX 7200's active tamper response will immediately destroy all sensitive information and cryptographic keys rather than exposing them.

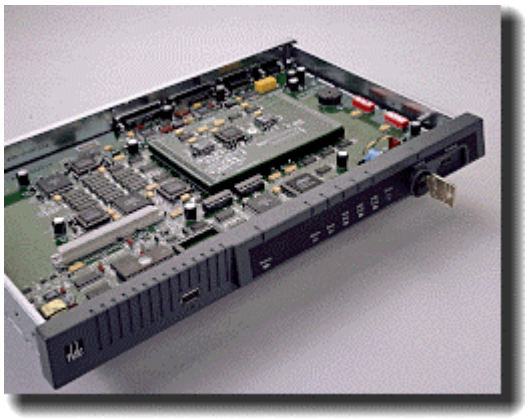


Figure 2 – The CipherX 7200 Features Active Tamper Response

The CipherX 7200 also features a pick-resistant Medeco™ front-panel lock, which prevents removal of the top panel and disables the front terminal access when locked.

2.2 Intuitive Interfaces

The front panel of the CipherX 7200 is shown in Figure 3. The front panel features the Terminal port, Lock, Erase button, diagnostic Light Emitting Diodes (LEDs), and a Fill port used for the secure loading of cryptographic keys with a TCC SmartModule. For more information on these interfaces and the LED diagnostics please refer to the CipherX 7200 User's Manual, FIPS Certification Submission document 1I or Section 3 of FIPS 140-1 certification Submission document 1G. The Status LEDs that are on the front panel are Power, Alarm, Error, Test Key, WAN Link, and Local Link.

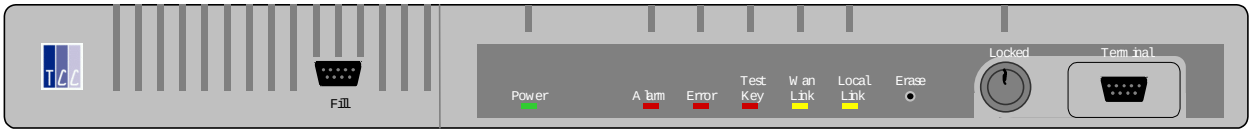


Figure 3 – The CipherX 7200 Front Panel

The rear panel of the CipherX 7200 provides the main communication interfaces as shown in Figure 4. There are two ethernet interfaces for the Local and WAN sides of the network (using either a 10BaseT or Attachment Unit Interface (AUI) interface), a Direct Current (DC) power port, and an auxiliary terminal ports. The auxiliary terminal provides an optional alarm relay output, and is used by the factory during assembly and testing. The rear panel also has two high-speed serial interface ports that are not used in the normal operation of the module. The DTE (Local) and DCE (WAN) ports are disabled by a hardware lockout.

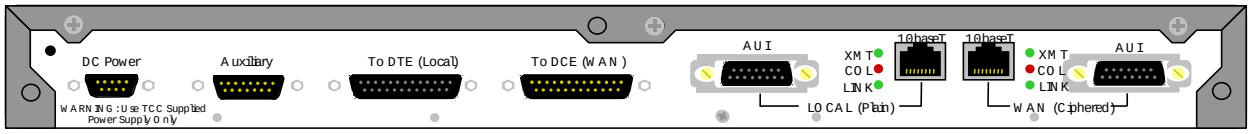


Figure 4 – The CipherX 7200 Rear Panel

The physical interfaces shown above provide the following logical interfaces into the module:

Panel	Physical Interface	Logical Interfaces
Rear	Power Supply	Power
Rear	Auxiliary Port	Status Output
Rear	To DTE (Local)	Not Used
Rear	To DCE (WAN)	Not Used
Rear	AUI (local)	Control Input, Data Input, Data Output, Status Output
Rear	10BaseT (local)	Control Input, Data Input, Data Output, Status Output
Rear	AUI (WAN)	Control Input, Data Input, Data Output, Status Output
Rear	10BaseT (WAN)	Control Input, Data Input, Data Output, Status Output
Rear	Status LEDs	Status Output
Front	Fill Port	Data Input, Data Output

Front	Terminal Port	Control Input, Data Input, Data Output, Status Output
Front	Lock	Control Input
Front	Erase Button	Control Input

Table 1 – Physical and Logical Interfaces

2.3 Secure Cryptography

The Cipher X 7200 supports 3-DES (Triple Data Encryption Standard) encryption to protect data packets and key management messages over the network. For network traffic the module uses 3-DES in the 64-bit Cipher Block Chaining (CBC) mode for optimum cryptographic throughput. Initialization vectors are negotiated real-time and provide a higher level of security.

2.3.1 Key Management

The Cipher X 7200 uses a three-tier key architecture for Key Management in compliance with the ANSI X9.19 standard, an update to replace ANSI X9.17. This approach provides high security and ease of use for both key generation and distribution to the module.
In a three-tier key architecture, there are three encrypting keys that are used to securely encrypt and distribute keys and data.

1. Data Encrypting Keys (DEKs) are used to encrypt all network traffic. DEKs are negotiated and electronically distributed between two modules, and are unique for each SA.
2. Key Encrypting Keys (KEKs) are used to protect (encrypt) DEKs. KEKs can be generated by the Module or by KEYNET. KEKs are shared by all devices in a Secure Community, and are used to determine which devices participate in each community. KEYNET provides the ability to automatically generate, distribute and manage KEKs over the network.
3. Master Key Encrypting Keys (MKEKs) are used to protect (encrypt) KEKs. MKEKs can be generated by the Module or by KEYNET. In FIPS 140-1 mode, the 7200 uses a split knowledge procedure to distribute MKEKs. Each half of an MKEK is written to a SmartModule, and is saved with a password to authenticate the key split.

Using KEYNET, the only key the operator needs to manually distribute is the MKEK. Once loaded, KEYNET and the Module will manage the generation and distribution of the KEKs, and DEKs.

2.3.2 Key Generation

All keys are generated using a pseudo-random algorithm defined in Appendix C of the document "American National Standard, X9.17-1985, Financial Institution Key Management (Wholesale), ...". entitled "Pseudorandom Key and IV Generator". Note: Because this algorithm requires a changing ‘Seed’ value in order to produce the random output, the Module samples a 16-bit internal timer four times to derive the 64 bit seed.
Message Authentication Codes (MACs) are used to authenticate encrypted data and key management messages. The MAC computation is performed as described in Appendix C of ANSI X9.19 “Procedure To Prevent Exhaustive Key Determination”.

2.3.3 Test Key

The Module also supports Test Key. Test Key is a factory installed KEK that is typically used for demonstration and performance evaluation. When test key is enabled, a front panel LED is lit indicating that Test Key is in use. Use of the Test Key to form secure associations is not permitted in secure operation of the module.

2.3.4 Security Policies

In order to determine which network traffic to encrypt, block or bypass, the operator will define a Security Policy for each device. When the Security Policy on two devices is set to cipher (encrypt) the Modules will negotiate a DEK and will establish a Secure Association (SA). If the policies do not match, the modules will not negotiate an SA and traffic will not pass. This approach provides added security, since both modules must be correctly configured and keyed in order to pass ciphered data. Note: KEYNET automates this process by providing the KEYNET operator with the ability to manage multiple devices with one Security Policy.

2.4 Roles

The CipherX 7200 supports identity-based authentication of its operators and provides two distinct roles: User and Crypto-Officer. In FIPS mode, only one Crypto Officer and one User will be defined.

> The operator assigned to the **User** role acts as a local administrator and is given access to the module diagnostics and the ability to view the module Configuration, Logs, and Statistics. However, the User role does not have the ability to read or modify any sensitive module information such as keying material. The User interfaces with the module using the Cipher Site Manager or KEYNET.
>
> The operator assigned to the **Crypto Officer** role has the responsibility for configuring security-sensitive information for the CipherX 7200, including keys, and IP addresses for secure tunnels. The Crypto Officer role has access to all services provided by the CipherX 7200, and maintains physical control of the keys to the front panel lock. The Crypto Officer interfaces with the module using the Cipher Site Manager or KEYNET (via Secure SNMP).

An operator authenticates to the module (using the Cipher Site Manager (CSM) application) by providing a password through a challenge-response protocol. Authentication and control input is through the terminal port after the Medeco™ key has been turned to the terminal position. The active User or Crypto Officer session is ended by exiting the CSM program, turning the key to the locked position, disconnecting the cable to the terminal, or powering down the module. Multiple invalid login attempts are logged security events and trigger a 10 second lockout timer that makes password attacks infeasible. Login is achieved via challenge-response; therefore, the password is never passed in the clear.

Authentication through the KEYNET module uses secure encryption with a Master Key Encryption Key (MKEK) per ANSI X9.17. Each command that is sent from KEYNET is authenticated. A separate password function is used to authenticate the loading of MKEKs from a SmartModule. The operator is requested to reenter a password to authenticate who entered the MKEK.

2.5 Services:

User Services: The Cipher Site Management (CSM) application allows the User to configure, manage, and obtain the status of each of the following functional areas of the CipherX: Configuration, Diagnostics, and SmartModule. These give the following services to the User:

Front Panel LED Status. (User Service) The front panel LEDs provide basic status indications to the operator of the module. As shown in Figure 3, there is a Power LED indicating power and battery status, a critical Alarm LED, a non-critical Error LED, a test key LED, and two bi-color LEDs for LAN and WAN link status. If an alarm or error occurs at start-up, the LEDs are used to indicate type of failure that occurred. The LED status can be viewed directly or by using CSM. Please refer to the CipherX 7200 User Manuals, Submission Document 1I, for a full description of the LEDs and their status indications.

View Alarms and Logs. (User Service) The security event logs can be viewed using CSM, including the alarms log, errors log, and security log. When an alarm occurs, all end-to-end network data at the DTE and DCE interfaces is blocked until the alarm condition is resolved and/or removed. When an alarm or error occurs, the appropriate LED is lit on the Front panel and an audible alarm is turned ON steady for an Alarm event and beeping for an Error event (if enabled by the Configuration/Parameters setting). The operator must either correct the alarm condition or view the error log before the audible alarm can be silenced.

Initialize SmartModule. (User Service) – The module will create a new header for the SmartModule and clear the data on the current module.

Status Services. (User Service) The user may view the setting of the DIP Switches (see section 4.1.1), view statistics on the packets sent and received by the module, Bypass mode status, and report the module firmware version.

Reset Module. (User Service) The module may be reset by issuing a command from the CSM. An operator may also use the erase button on the front panel to erase and reset the module (see below). The module may also be reset by removing external power to the device momentarily.

Zeroize. (User Service) Zeroization may be triggered by pressing the erase button on the front panel. The button is recessed behind the Front Panel and is activated by inserting a thin object (e.g. paper clip or pen point) through the $^1/_8$" hole.

View and Configure Parameters. (User Service). The User may view the unit operational parameters, including Unit ID, Alarm Sound, Module Clock, SNMP management addresses, Promiscuous Mode for NICs, and Network and Transport protocols allowed.

On-Demand Test – (User Service) The user is able to request specific self-test be performed at any time. CSM provides a Diagnostics window which provides the operator with a list of tests and check boxes to select the tests. After the test are selected the operator selects the Start Tests button.

Crypto Officer Services: In addition to the services that are provided to the 'User', the module makes the following services available to the 'Crypto Officer':

Encryption/Decryption - (Crypto Officer Service) IP packets are encrypted or decrypted with a DEK established for a particular session. The Crypto Officer specifies which IP address ranges are to be encrypted using the module's Security Policy Table. Once configured, subsequent IP packets are individually processed and encrypted or decrypted by the module for the Crypto Officer.

Change Password. (Crypto Officer Service) The Crypto Officer sets the passwords for both the Crypto Officer and the User. The CipherX modules are initially configured with a default password of "guest". Passwords may be changed either locally by the Crypto Officer, or remotely via KEYNET. Existing Passwords may never be displayed either locally or at KEYNET.

Key Management. (Crypto Officer Service) The Crypto Officer can load MKEKs and Key Encrypting Keys (KEKs), change Data Encrypting Keys (DEKs), set up automatic changes for DEKs and KEKs, view which keys loaded, and load test keys into the module. Keys can be loaded through the local fill port with SmartModules, or using KEYNET Manager. MKEKs must always be distributed via SmartModule, while KEKs may be distributed using ANSI X9.17. Test keys can be used to set up a special Security Association (SA) with another device configured with the test key in place of a randomly generated DEK. The use of test keys is indicated via a special LED on the front panel.

SmartModule. (Crypto Officer Service) When a SmartModule is connected to the module's fill port, the Crypto Officer may view the contents of a SmartModule, load items contained in the SmartModule into the module, or create and store items into a SmartModule. When in FIPS mode the keys can not be viewed.

Configure Security Policy Table. (Crypto Officer Service) The Crypto Officer may configure access controls for pairs of source and destination IP nodes, networks, and subnetworks through the Security Policy Table. This table is used to define which traffic sources are plaintext, encrypted, or blocked. The module provides capabilities for blocking, bypassing, or processing packets based on transport layer in addition to flexible management of broadcast frames.

Firmware Upgrade. (Crypto Officer Service) The Crypto Officer may download new firmware for installation on the CipherX 7200. Only firmware that has been digitally signed by TCC using a triple-DES Message Authentication Code (MAC) will be accepted and installed by the module. The CipherX uses the X9.19 MAC.

Manage Secure Associations. (Crypto Officer Service) Management of *Secure Associations* and configuration data is done by the local CipherX 7200 operator or remotely via TCC's KEYNET Central Management system. Industry-standard

management systems (i.e.. HP Openview) may access the MIB II section of the CipherX 7200.

Front Panel Keyswitch. (Crypto Officer Service) The Crypto Officer maintains physical control of the keys to the Medeco™ lock that turns the keyswitch from locked to terminal. The locked position physically locks on the top cover of the module and disables access through the terminal port.

Zeroize. (Crypto Officer Service) A Crypto Officer only service, zeroization is available to selectively erase the MKEK, change DEKs, or overwrite KEKs. As described above complete user zeroization is also available.

Secure SNMP Management. (Crypto Officer Service) The SNMP application includes an SNMP agent that allows KEYNET to securely query the unit for information and to set database values remotely. Processing requirements, and format for KEYNET to device SNMP Messages are completely described in *Functional Specification: KEYNET.*

Bypass Mode. (Crypto Officer Service) The Crypto Officer has privileges to transition the module into bypass mode from the controls in CSM or KEYNET. In bypass mode, all IP traffic will be passed through the CipherX without encryption.

2.6 Alarms and Errors

The CipherX defines both Alarms and Errors for recording problems with the system or processing. An Alarm is a condition that violates the unit's ability to reliably and securely process user data. Therefore, when an alarm occurs, all end-to-end network data at the LOCAL and WAN interfaces is blocked until the alarm condition is removed. Alarms, when they first occur, have persistence. This means that they are always ***active*** until the operator either corrects the problem or resets the unit. Alarms are never 'self-healing'.

The module will indicate either fatal or operational alarms and detected errors with the LEDs, audible alarm warning, and logged error entries. The CipherX module defines a state for each of these alarm types. When a Fatal Alarm occurs, the module will transition to the appropriate state and stop all network traffic from being processed. When an Operational alarm is active, the unit is fully functional, however a command will be sent to the DSP Processor to immediately clear all Security Associations.

Errors are events that occur during system operation that are not normal but do not affect the unit's ability to process user data in a secure manner. While this may affect activity on a single Security Association, network activity in general is not affected. All Errors have transient applicability, meaning that they occur at some instant in time, and then (possibly after some software action) are immediately considered historical. Thus, there is no such thing as an ***active*** Error.

When an error occurs, the Error LED is lit on the front panel, and the event is recorded in the internal Error Log which the operator may view through the Cipher Site Manager interface. In

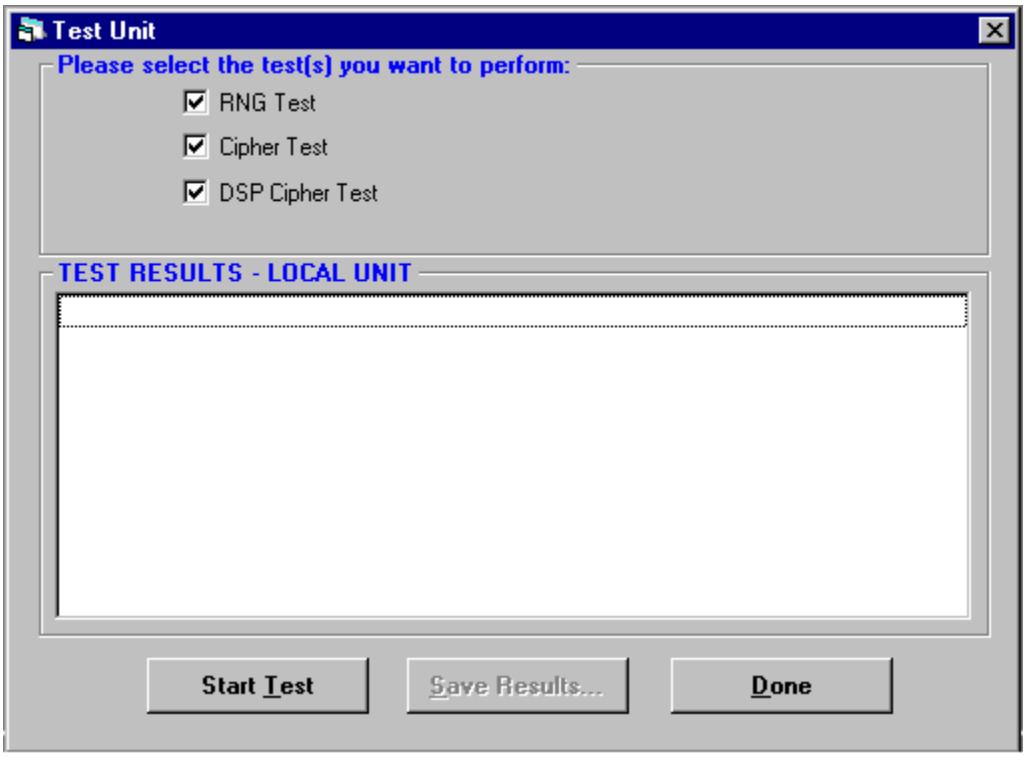
addition, if enabled via configuration, the audible alarm is turned on intermittently beeping (1 second on, 1 second off) for an Error.

3 Self-Tests

The embedded application in the CipherX products contains a set of built-in diagnostics that are run in a variety of modes. The full suite of diagnostics are run when the unit is booted. The front panel LEDs are used to display the status of those diagnostics. A portion of these diagnostics can be run from the CSM. The CipherX performs the following self-test at start-up:

- Host SHA1 Known Answer Test
- Host TDES Known Answer Test
- Host MAC Known Answer Test
- DSP TDES Known Answer Test
- Host ROM Test
- DSP ROM Test
- Host RNG test – Performs the following Statistical RNG tests: Monobit test, Poker test, Long Runs test, Runs test
- Host Cipher Test
- Host RAM Test
- DSP RAM Test
- Bypass mode Test

The Statistical Random Number Generator, Cipher, and DSP Cipher tests can all be run on—demand from the menu bar under Diagnostic – Test. The Test Unit window is displayed and the operator can select which test will be run. The test results are displayed in the lower half of the Test Unit window.



Other Self-test are run conditionally such as the Firmware Upgrade check and the Continuos Random Number Generator (RNG) test. The Firmware Upgrade test validates the firmware that is loaded by performing a MAC of the firmware and comparing it to a MAC sent with the upgrade from TCC. A 64-byte "shared secret" pad will be appended to the upgrade file before the MAC is performed. The "shared secret" will be written to the CipherX during manufacturing at the factory. The firmware upgrade is verified when the two MACs, each using the "shared secret", match. The continuous RNG test is run every time a number is requested from the RNG. The module stores the previously generated 64 bits and compares them to the next 64-bits generated.

If any of the self-test fail during start-up or during an on-demand call, the module transitions to a Fatal Alarm State and stops all network communication. When a self-test causes a Fatal Alarm, the operator can log on to view the error logs and diagnose the problem.

4 Secure Operation of the Module

The CipherX has the capability of operating in FIPS-mode and non-FIPS mode. Therefore, it is critical to insure all the unit's configurations are correct for FIPS-mode if that is the expected mode of operation. A number of physical and procedural configurations are required to operate the Cipher X 7200 in a FIPS 140-1 compliant manner.

- All keys saved to the SmartModule must be either encrypted or utilize split knowledge procedures.
- The MKEK should NOT be loaded by any other means than from a SmartModule.
- Cipher Site Manager should NOT be used to enter KEKs into the module.
- The Test Key should not be used to form secure associations.
- Only one Crypto Officer and one User should be defined.
- DIP switch and Jumper settings should be set as described in Section 4.1 of this document. This is how the system is shipped from the TCC factory.
- The default password for both the Crypto Officer and the User should be changed when first installing the device.

Validating that these procedures and configuration are correct will insure that that TCC module provides the full security of a level 3, FIPS 140-1 certified module.

4.1 Jumpers and DIP switches

The CipherX 7200 has several Dual In-Line Package (DIP) switches and jumpers internal to the device that are factory set for FIPS 140-1 compliant operation. However, like modifications to any part of the module's internal hardware, these jumpers and DIP switches affect secure operation of the CipherX 7200. They are described here for reference and comparison purposes when tampering is suspected. Incorrect configuration of the jumpers and DIP switches could cause module malfunction and changing factory default settings is not recommended.

4.1.1 DIP Switch Settings

A set of DIP switches located inside the unit (shown in Figure 5) configure certain hardware options for the module.

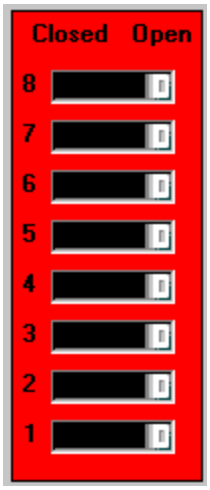


Figure 5 – DIP Switch Settings in the CipherX 7200

The Cipher Site Manager or KEYNET application will read and display the current setting of the DIP switches to the operator. The module is factory configured for FIPS 140-1 compliant operation with the following settings:

Table 2 – FIPS 140-1-mode DIP switch settings

Switch	Description	FIPS 140-1 Mode Setting
1	Key Management Mode	OPEN
2	MKEK erase	OPEN
3	FIPS Mode	OPEN
4	Test Key	OPEN
5	Spare – not used	OPEN
6	Key Generation	OPEN
7	Spare – not used	OPEN
8	Factory Test	OPEN

Note: When the FIPS 140-1 mode is selected via DIP switch, some Key Generation options change. In FIPS mode, MKEKs are only written to SmartModule in Split format. The operator is prompted to select Passwords for each half of the Split Key. The entered Password is processed together with the MKEK half and the encrypted result is stored in the SmartModule. In order to load the MKEK half, the Crypto Officer must first enter the password encrypted with the MKEK during generation.

4.1.2 Jumper Settings

The following internal jumpers settings are important to the FIPS mode of operation.

Jumper Options		
JU14 & JU17	*A-C B-C	Normal RAM Erasable(RAM bank 1) All RAM Erasable
JU16	*A-C B-C	Normal Battery Power Master Erase(Factory Only)
JU18	*A-C B-C OUT	LOCKED Front Panel Key Erase UNLOCKED Front Panel Key Erase Front Panel Key Erase Disabled
JU22	*IN OUT	Beeper Enabled Beeper Disabled

*Note : * indicates the delivered configuration.*