

# **Security Policy for CypherCell ATM Encryptor**

## **Compliant to FIPS PUB 140-1**

**Copyright Ó2001 CTAM Pty. Ltd.  
ACN 080 481 947**

**Reproduction is authorised provided  
the security policy is copied in its entirety.**

**Version**

Version 2.1      21 November 2001  
Release of non-proprietary version 2.1 of CypherCell Security Policy

## Table Of Contents

<b>1. INTRODUCTION .....</b>	<b>4</b>
1.1 OVERVIEW .....	4
1.2 IDENTIFICATION .....	4
1.3 FIPS PUB 140-1 SECURITY LEVEL .....	6
1.4 REFERENCES .....	6
1.5 GLOSSARY OF KEY TERMS.....	6
<b>2. CYPHERCELL DESCRIPTON .....</b>	<b>8</b>
2.1 OVERVIEW .....	8
2.2 EXTERNAL INTERFACES .....	10
<b>3. SECURITY ENVIRONMENT.....</b>	<b>11</b>
3.1 ASSUMPTIONS .....	11
3.2 THREATS.....	13
3.3 ORGANISATIONAL SECURITY POLICIES .....	13
<b>4. CYPHERCELL ROLES AND SERVICES .....</b>	<b>14</b>
4.1 REMOTE MANAGEMENT ACCESS SECURITY POLICY.....	14
4.1.1 Identification and Authentication Policies .....	14
4.1.2 Identity Based Access Control.....	14
4.2 LOCAL MANAGEMENT ACCESS SECURITY POLICY.....	18
4.2.1 Identification and Authentication Policies .....	18
4.2.2 Identity Based Access Control.....	18
4.3 CONFIGURATION ROLE.....	21
4.4 USER ROLE.....	22
4.5 NETWORK USER SERVICES .....	23
4.6 SECURITY POLICY ENFORCING FUNCTION SUMMARY .....	25
<b>5. PHYSICAL SECURITY POLICY.....</b>	<b>27</b>
<b>6. INITIALISATION POLICY .....</b>	<b>27</b>
<b>7. FIRMWARE UPGRADE POLICY.....</b>	<b>31</b>
<b>8. CRYPTOGRAPHY .....</b>	<b>31</b>
8.1 CRYPTOGRAPHIC ALGORITHMS .....	31
8.2 KEY MANAGEMENT .....	31
8.3 KEY GENERATION.....	32
8.4 PRIVATE/PUBLIC KEY AND USER PASSWORD PROTECTION.....	32
<b>9. SELF -TESTS .....</b>	<b>32</b>
<b>10. FIPS PUB 140 -1 MODE OF OPERATION .....</b>	<b>32</b>

# 1. INTRODUCTION

## 1.1 Overview

This document provides a complete and consistent statement of the security policy of CypherCell, a high-speed ATM security module.

The Security Policy details the module's security requirements and the countermeasures proposed to address the perceived threats to the assets protected by the module.

## 1.2 Identification

### CypherCell ATM Encryptor - Firmware Version 2.1.0, Hardware Revision 3

The following interface and power supply configurations are available. The interface and power supply configurations combinations are excluded from the requirements of FIPS 140-1 because they do not affect the secure operation of the module. The tamper-evident seals, as outlined in this document, protect these different configurations ensuring that the cryptographic boundary's physical security is maintained

Description
OC3/STM-1 Multimode Fibre Network Interface OC3/STM-1 Multimode Fibre Local Interface DES Algorithm 155Mbps throughput 1024 virtual circuits 110 to 240VAC  OC3/STM-1 Singlemode Fibre Network Interface OC3/STM-1 Singlemode Fibre Local Interface DES Algorithm 155Mbps throughput 1024 virtual circuits 110 to 240VAC
OC3/STM-1 Singlemode Fibre Network Interface OC3/STM-1 Multimode Fibre Local Interface DES Algorithm 155Mbps throughput 1024 virtual circuits 110 to 240VAC
OC3/STM-1 Multimode Fibre Network Interface OC3/STM-1 Multimode Fibre Local Interface DES Algorithm 155Mbps throughput 1024 virtual circuits 24 to 48VDC
OC3/STM-1 Singlemode Fibre Network Interface OC3/STM-1 Singlemode Fibre Local Interface DES Algorithm 155Mbps throughput 1024 virtual circuits 24 to 48VDC
OC3/STM-1 Singlemode Fibre Network Interface OC3/STM-1 Multimode Fibre Local Interface DES Algorithm 155Mbps throughput 1024 virtual circuits 24 to 48VDC
T3 BNC Network Interface T3 BNC Local Interface DES Algorithm 45Mbps throughput 1024 virtual circuits 110 to 240VAC

Description
E3 BNC Network Interface E3 BNC Local Interface DES Algorithm 34Mbps throughput 1024 virtual circuits 110 to 240VAC
E1 BNC Network Interface E1 BNC Local Interface DES Algorithm 2Mbps throughput 1024 virtual circuits 110 to 240VAC
T1 RJ45 Network Interface T1 RJ45 Local Interface DES Algorithm 1.5Mbps throughput 1024 virtual circuits 110 to 240VAC
T3 BNC Network Interface T3 BNC Local Interface DES Algorithm 45Mbps throughput 1024 virtual circuits 24 to 48VDC
E3 BNC Network Interface E3 BNC Local Interface DES Algorithm 34Mbps throughput 1024 virtual circuits 24 to 48VDC
E1 BNC Network Interface E1 BNC Local Interface DES Algorithm 2Mbps throughput 1024 virtual circuits 24 to 48VDC
T1 RJ45 Network Interface T1 RJ45 Local Interface DES Algorithm 1.5Mbps throughput 1024 virtual circuits 24 to 48VDC

### 1.3 FIPS PUB 140-1 Security Level

CypherCell meets the overall requirements applicable to FIPS PUB 140-1 Level 2. It meets the requirements as a multi-chip standalone module.

Security Requirements Section	Level
Cryptographic Module	3
Module Interfaces	3
Roles and Services	3
Finite State Machine	3
Physical Security	2
EFP/EFT	N/A
Software Security	3
Operating System Security	N/A
Key Management	3
Cryptographic Algorithms	3
EMI/EMC	3
Self Test	3

### 1.4 References

1. FIPS 140-1 Security Requirements for Cryptographic Modules January 11, 1994
2. Derived Test Requirements for FIPS PUB 140-1, Security Requirements for Cryptographic Modules
3. FIPS 46-2 Data Encryption Standard
4. FIPS 46-3 Data Encryption Standard
5. FIPS 81 DES Modes of Operation
6. FIPS 181-1 Secure Hash Standard
7. AF-SEC-0100.00 ATM Forum Security Specification Version 1.0 February 1999
8. RFC2574 User-based Security Model for version 3 of the Simple Network Management Protocol The Internet Society – April 1999
9. RFC2459 Internet X.509 Public Key Infrastructure – January 1999
10. Public Key Cryptography Standards #1 (PKCS #1), “RSA Encryption Standard,” RSA Laboratories, Version 1.5, November 1993 (Also available as RFC2313, March 1998).

### 1.5 Glossary of Key Terms

ATM	Asynchronous Transfer Mode
CLP	Cell Loss Priority
DES	Data Encryption Standard
GFC	Generic Flow Control
HEC	Header Error Check
MASTER KEY	Key used to encrypt session keys
MBPS	Megabits per second
MIB	Management Information Block
OAM	Operation and Maintenance management cells
OID	Object Identifier
OSP	Organisational Security Policy
PTI	Payload Type Indicator
PVC	Permanent Virtual Circuit
PVP	Permanent Virtual Path
RFC	Request for Comment

RSA	Public Key Algorithm
SEF	Security Enforcing Function
SESSION KEY	Key used to encrypt the payload of an ATM cell
SFP	Security Function Policy
SNMPv3	Simple Network Management Protocol Version 3
TOE	Target of Evaluation
TSF	TOE Security Function
TSP	TOE Security Policy
UAT	User Account Table
VCAT	Virtual Channel Action Table
VC	Virtual Circuit
VP	Virtual Path
VPI/VCI	Virtual Path Identifier/Virtual Channel Identifier
X.509	Digital Certificate Standard RFC 2459

## 2. CYPHERCELL Description

### 2.1 Overview

CypherCell is a high-speed encryptor specifically designed to secure voice, data and video information transmitted over Asynchronous Transfer Mode Networks (ATM) at data rates from 1.5Mbps to 155Mbps.

CypherCell provides confidentiality of the transmitted information by encrypting the 48-byte payload of the ATM cell but leaving the five-byte ATM header unchanged, which enables switching of the cell through ATM networks. The format of an ATM Cell is shown in Figure 1.

GFC	VPI	VCI	PTI	CLP	Checksum	Payload
4 bits	8 bits	16 bits	3 bits	1 bit	8 bits	48 bytes

Figure 1 - ATM Cell Format

CypherCell is a multi-chip standalone cryptographic module with the outer casing defining the cryptographic boundary. The steel case completely encloses CypherCell to protect it from tampering. Any attempt to remove the top cover will automatically erase all sensitive information stored internally in the encryptor.

CypherCell provides access control and authentication between secured sites and confidentiality of transmitted information by cryptographic mechanisms. The unit can be added to an existing ATM network with complete transparency to the end user and network equipment. An example installation of the CypherCell encryptor is shown in Figure 2.

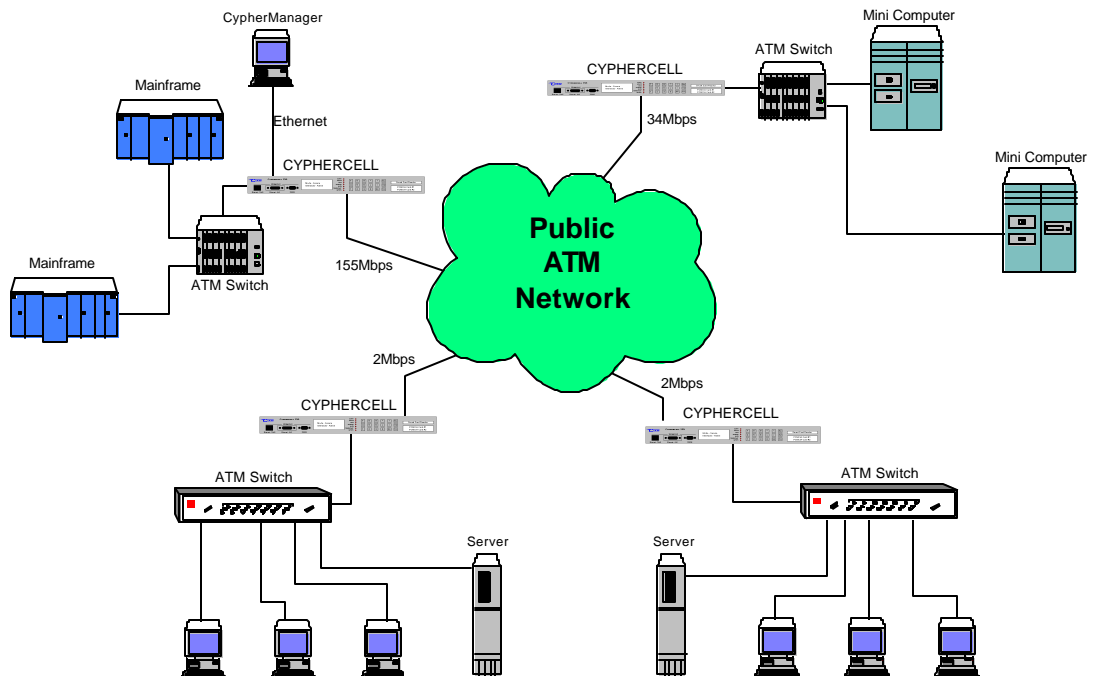


Figure 2 – A Secure ATM Network

CypherCell supports single or triple 2/3 key DES in cipher feedback mode.

Any combination of encrypted or unencrypted virtual circuits can be configured up to a maximum of 65,536 active connections. Each encrypted virtual circuit uses different encryption keys. Any Virtual Path Identifier/Virtual Channel Identifier (“VPI/VCI”) combination can be mapped to one of the 65,536 available connections. Support is provided for both Permanent Virtual Paths (“PVP”) and Permanent Virtual Circuits (“PVC”) modes of operation.



Operation and Maintenance (“OAM”) cells and PVP cells with VCI values of 0 to 31 can be selectively excluded from the encryption process enabling full ATM network management functions to be maintained. Virtual circuits with these VCI addresses must not be used for user data.

Key management and authentication are based on the ATM Forum Security Specification Version 1.0 and use RSA public key cryptography and X.509 certificates providing a fully automated key management system. Master keys and initial session keys are transferred between encryptors using X.509 certificate authenticated RSA public key cryptography. Session key updates are transferred between encryptors using the master key and SHA-1 and can be set to change according to time or the number of cells encrypted.

CypherCell provides access control by discarding cells if the access rules for that particular virtual circuit are violated. Access controls may be set for any VPI/VCI as encrypt, bypass (all cells pass through unaltered) or discard with an additional control that discards cells that violate defined times of access.

CypherCell connects to the local and remote network using SONET OC-3c/STM1 multimode/single mode fibre, a T3, E3 or E1 BNC coaxial connection or T1 RJ45 connection. When operating at full bandwidth, CypherCell will not discard any valid cells for all modes of operation.

CypherManager, which uses SNMPv3 management sessions, provides secure remote management of the unit. Depending on the network security policy, an operator may be required to have both an authentication password and a privacy password for remote management sessions. By default, CypherManager enforces the requirement for authentication passwords, and privacy passwords are enabled at the option of the CypherCell/CypherManager administrator. The dedicated Ethernet management port on CypherCell supports 10BaseT and AUI connections.

Local management is also available via an RS232 port supporting a command line interface. Using a basic terminal emulator, an operator is required to present their user name and authentication password directly to the CypherCell encryptor before a local management session is allowed. Operators of the module cannot use the local management RS232 port to initialize the CypherCell encryptor with an X.509 certificate. This functionality is restricted to SNMPv3 management sessions.

CypherCell supports different types of operator roles with different privileges according to a set of pre-defined roles. The four defined Crypto-Officer roles are Administrator, Supervisor, Operator, and Configure and a Maintenance role called Crypto-Maintain. The one defined User Role is Network User Services, which is another encryptor requesting a secure connection.

Only the Crypto-Officer Administrator has unrestricted access to the security features of the CypherCell encryptor which include viewing all configuration parameters, audit logs, and status, adding, modifying, and deleting entries to the UAT and VCAT tables, installing signed X.509 certificates, clearing audit logs, and modifying configuration parameters. No other defined role can activate X.509 certificates, which are required for CypherCell to commence operation.

The Crypto-Officer Supervisor roles are a subset of the Crypto-Officer Administrator roles excluding activating X.509 certificates, adding, modifying, and deleting entries to the UAT table, and clearing the audit logs.

The Crypto-Officer Operator can only view all configuration parameters, audit logs, and status.

The Crypto-Officer Configure role can change the local and network interface modules and the power supply input voltage.

The Crypto-Maintain role is mainly for installing firmware upgrades but they can view all configuration parameters, audit logs, and status.

The Network Services User role is to provide cryptographic services to ATM cells received and transmitted to another encryptor on the local and network interfaces for specified virtual circuits.

CypherCell provides an audit capability to support the effective management of the security features of the device. The audit capability records all management activity for security relevant events.

Any organization using the CypherCell encryptor should ensure that an appropriate operational environment is maintained that satisfies those assumptions listed in section 3.1 of this Security Policy.

## 2.2 External Interfaces

CypherCell is housed in a steel case that is compatible with 19inch rack systems and is 1 rack unit in height.



The front panel interfaces are:

- RJ45 connector for remote management via an IP/Ethernet based network
- AUI connector for remote management via an IP/Ethernet based network  
(Note: only one of the Ethernet connections can be active at a time)
- DB9 RS232 connector for local configuration by a console
- Nine indicators show the status of internal functions of the unit. The indicators are either red, orange or green or flashing depending on the status of the function
- Two line display for operator output
- Keypad for operator input
- Two PCMCIA slots that are used for program upgrades.
- Smartcard reader. The smart card reader is disabled and does not provide any functionality.



The rear panel interfaces are:

- Local OC3-c/STM-1 fiber connector, BNC coaxial or RJ45 connectors for connection to the protected network.
- Network OC3-c/STM-1 fiber connector, BNC coaxial or RJ45 connectors for connection to the unprotected network. (This interface connects to the far end encryptor).

The rear panel also has a power entry module for connection of the unit to electrical power. Loss of electrical power results in the destruction of all DES keys used to secure the transmitted information.

A tamperproof seal is also placed across the join between the top cover and the bottom of the chassis, as shown above. Any attempt to remove the top cover will destroy the integrity of the tamperproof seal.

CypherManager is a Windows based application that is used to securely remotely manage CypherCell encryptors. It presents to operators a Graphical User Interface (GUI), which is used to set and monitor the CypherCell internal configuration parameters. CypherManager communicates with CypherCell encryptors using SNMPv3 commands over an IP/Ethernet network. The IP/Ethernet network connects to CypherCell using the RJ45 or AUI connector on the front panel of the encryptor or via the local and network interfaces where the SNMPv3 commands are extracted from a designated VCI.

### 3. Security Environment

#### 3.1 Assumptions

CypherCell is intended for use in organizations that need to provide confidentiality of information transmitted over ATM networks and access control to prevent unauthorized connection to the protected ATM network. The following assumptions about the operating environment and intended use of the CypherCell and CypherManager apply.

##### **A.CERTIFICATE**

Each unit has a valid X.509 certificate loaded into the unit before commencement of secure operation. The CypherCell encryptor cannot operate securely without a valid X.509 certificate loaded in the module.

##### **A.PRIVATEKEY**

It is assumed that a password used to protect the private key of the CypherManager remote management station is restricted to only Crypto-officer Administrators of the CypherCell ATM encryptor. Operators other than Crypto-officer administrators could attempt to use the key to sign X.509 certificate requests, if they could recover the CypherManager private key.

##### **A.ENCRYPTION**

Only encryption of the ATM cell payloads is required and that single DES or TDES in cipher feedback mode is appropriate for the classification of information to be protected.

##### **A.KEYEXCHANGE**

It is assumed that a communications pathway exists for each virtual circuit or path, for automated key exchange using RSA public key cryptography, to transfer an initial master key and session key between units, and that RSA public key cryptography is appropriate for transfer of keys between units. Exchange of session keys, based on time or number of cells encrypted, is set in accordance with the defined network security policy.

##### **A.AUTHENTICATE**

It is assumed that X.509 certificate based authentication is appropriate for authentication of RSA key exchange. Correctly implemented X.509 certificate based authentication provides a stronger authentication mechanism than password based authentication mechanisms.

##### **A.ACCESS**

Access control rules on the cell traffic, determined by the VPI/VCI address, which forms part of the cell header are defined, and that the rules to be applied are configured for each VPI/VCI address value and set in accordance with the defined network security policy. Defining access control rules that do not comply with the defined network security policy may result in an insecure network.

The access control rules that can be applied are encrypt, bypass (the cell passes through unchanged) or discard. Additionally, for each VPI/VCI address an access time period can be set with cells received outside this time period being discarded.

##### **A.AUDIT**

It is assumed that appropriate audit logs are maintained and regularly examined in accordance with network security policy. Without capturing security relevant events or performing regular examination of audit records, a compromise of security may go undetected.

##### **A.ROLES**

It is assumed there is an administrator who is responsible for controlling who has access to the unit for configuration and monitoring activities through use of defined roles. There are five roles:

Crypto-officer administrator	who has full access rights;
Crypto-officer supervisor	who has full access rights except they cannot add, delete or modify user accounts, they cannot install X.509 certificates or delete audit logs; and
Crypto-officer operator	who can view all available information, except passwords of the other Crypto-officers, but cannot delete, add or modify the information.
Crypto-officer configure	who can change the local and network interface modules and the power supply input voltage.

Crypto-Maintain who can install firmware upgrades and view all available information but cannot delete, add or modify the information.

Each user is allocated a user name and authentication and privacy passwords and an appropriate role. Having defined roles provides a means of limiting access to security functions of the module to only those authorized operators who need to access those security functions.

#### **A.MANAGEMENT**

It is assumed that a console port or remote secure SNMPv3 management station is provided for managing the security features of the module. A means of securely managing the module must be provided to control its security features.

#### **A.INSTALL**

It is assumed that CypherCell is installed between the secure local ATM switch and an insecure network switch. CypherCell needs to be installed between a secure ATM switch and the insecure ATM network to ensure confidentiality of transmitted information.

#### **A.REMOTEMANAGEMENT**

It is assumed that only the CypherManager management station is used for remote management of CypherCell. If remote management is required then the dedicated Ethernet management port on the unit must be connected to an IP network that has connectivity to the management station. If inband management is enabled the encryptor connected to CypherManager can act as a gateway to the other encryptors in the secure network as long as a virtual connection is configured between the gateway encryptor and the other encryptors in the network.

It is assumed that CypherManager will be installed on a PC with the following minimum system configuration:

- Windows 95/98/NT4.0/2000 or higher
- 166MHz or higher speed processor
- 64MB of memory
- Hard disk drive with a minimum of 5MB of available application space
- CD drive for installation
- 3.5" floppy drive for (for RSA private key backup)
- SVGA or better display resolution
- Mouse or other pointing device
- Network adapter card
- TCP/IP connectivity

#### **A.SNMP**

It is assumed that the IP network connected to the dedicated Ethernet management port is capable of passing the SNMPv3 packets used to securely manage remote CypherCell encryptors.

#### **A.PEER**

Any other systems with which the module communicates are assumed to operate under the same security policy constraints, otherwise the confidentiality of the information sent to/from a remote instance of the module could not be assured.

#### **A.LOCATE**

It is assumed that the CypherCell is located in a secure area at the boundary of the site to be protected. It is required to be in a secure area to ensure that the unit is not physically bypassed.

#### **A.CYPHERMANAGER**

CypherManager is assumed to be located within controlled access facilities, which will aid in preventing unauthorized operators from attempting to compromise the security functions of the module. For example, unauthorized physical access to the private key used to sign CypherCell X.509 certificates.

#### **A.ADMIN**

It is assumed that one or more Crypto-officer administrators, together with any other Crypto-officer supervisors or Crypto-officer operators, who are assigned as authorized operators are competent to manage the module and who can be trusted not to deliberately abuse their privileges so as to undermine security.

### 3.2 Threats

This section identifies the threats, which CypherCell is designed to counter.

<b>T.CAPTURE</b>	An attacker may eavesdrop on or otherwise capture data being transmitted across a public ATM network in order to recover information that was to be kept confidential.
<b>T.CONNECT</b>	An attacker (insider or outsider) may attempt to make unauthorized connections to another ATM network and transmit information that was to be kept confidential, to another destination.
<b>T.ABUSE</b>	An undetected compromise of information may occur as a result of an authorized user of the module (intentionally or otherwise) performing actions the individual is authorized to perform.
<b>T.ATTACK</b>	An undetected compromise of information may occur as a result of an attacker (insider or outsider) attempting to perform actions that the individual is not authorized to perform.
<b>T.LINK</b>	An attacker may be able to observe multiple uses of services by an entity and, by linking these uses, be able to deduce information, which the entity wishes to be kept confidential.
<b>T.OBSERVE</b>	An attacker could observe the legitimate use of the remote management service by an authorized user when that authorized user wishes their use of that remote management service to be kept confidential.
<b>T.PHYSICAL</b>	Security critical parts of the module may be subject to physical attack, which may compromise security.
<b>T.PRIVILEGE</b>	A compromise of information may occur as a result of actions taken by careless, willfully negligent or hostile administrators or other authorized operators.

### 3.3 Organisational Security Policies

<b>P.CRYPTO</b>	All encryption services including, confidentiality, authentication, key generation and key management, must conform to standards specified by NIST.
<b>P.FILTER</b>	Traffic flow is controlled on the basis of the information in the ATM cell header, the Virtual Channel Action Table and the granting, by an authorized user, of explicit access controls. Any ATM cells, for which there is no VCAT entry, are discarded. By default, all ATM cells are discarded. This Organisational Security Policy must conform to the <i>Cell Control SFP</i> enforced by the module as defined in section 4.3. The P.FILTER OSP ensures that the correct protective action is applied to any given ATM cell received by the module.
<b>P.ROLES</b>	Administration of the module is controlled through the definition of roles, which assign different privilege levels to different types of authorized operators (administrators, supervisors, and operators). This Organisational Security Policy must conform to the <i>Remote Management Access Control SFP</i> and the <i>Local Management Access Control SFP</i> enforced by the module as defined in section 4.1 and 4.2. The P.ROLES OSP ensures that administration of the module is performed in accordance with the concept of <i>least privilege</i> .

## 4. CypherCell Roles and Services

### 4.1 Remote Management Access Security Policy

The Remote Management Access SP is used to protect the User Account Table (UAT), the Virtual Channel Action Table (VCAT) and other configuration parameters from unauthorized modification.

#### 4.1.1 Identification and Authentication Policies

The UAT table contains a list of operator accounts. Operators listed in the User Account Table (UAT) have access to the internal configuration parameters in the encryptor. Operators are identified by a unique user name. Authentication for each operator is achieved by the use of an authentication password.

For SNMPv3 remote access the user name, authentication and privacy passwords are used as specified in RFC2274.

For each operator the following security information is specified:

- User name
  - User authentication password
  - User privacy password
  - User role
  - Account Active/Inactive
- Note: Access is denied if the account is inactive.

Refer to section 10 for a description of FIPS PUB 140-1 Mode of Operation.

#### 4.1.2 Identity Based Access Control

The roles that can be assigned to an operator who has remote management access privilege are Crypto-officer Administrator, Crypto-officer Supervisor, Crypto-officer Operator or Crypto-Maintain.

All roles can view the UAT (except for user passwords) and VCAT tables and configuration parameters.

Actions that can be performed by each role are:

##### Crypto-officer Administrators

- View all configuration parameters
- View audit log
- View status
- Add, modify and delete entries to the UAT table
- Add, modify and delete entries to the VCAT table
- Install signed X.509 certificates
- Clear the audit log
- Modify configuration parameters

##### Crypto-officer Supervisors

- View all configuration parameters
- View audit log
- View status
- Add, modify and delete entries to the VCAT table
- Modify configuration parameters

##### Crypto-officer Operators

- View all configuration parameters
- View audit log
- View status

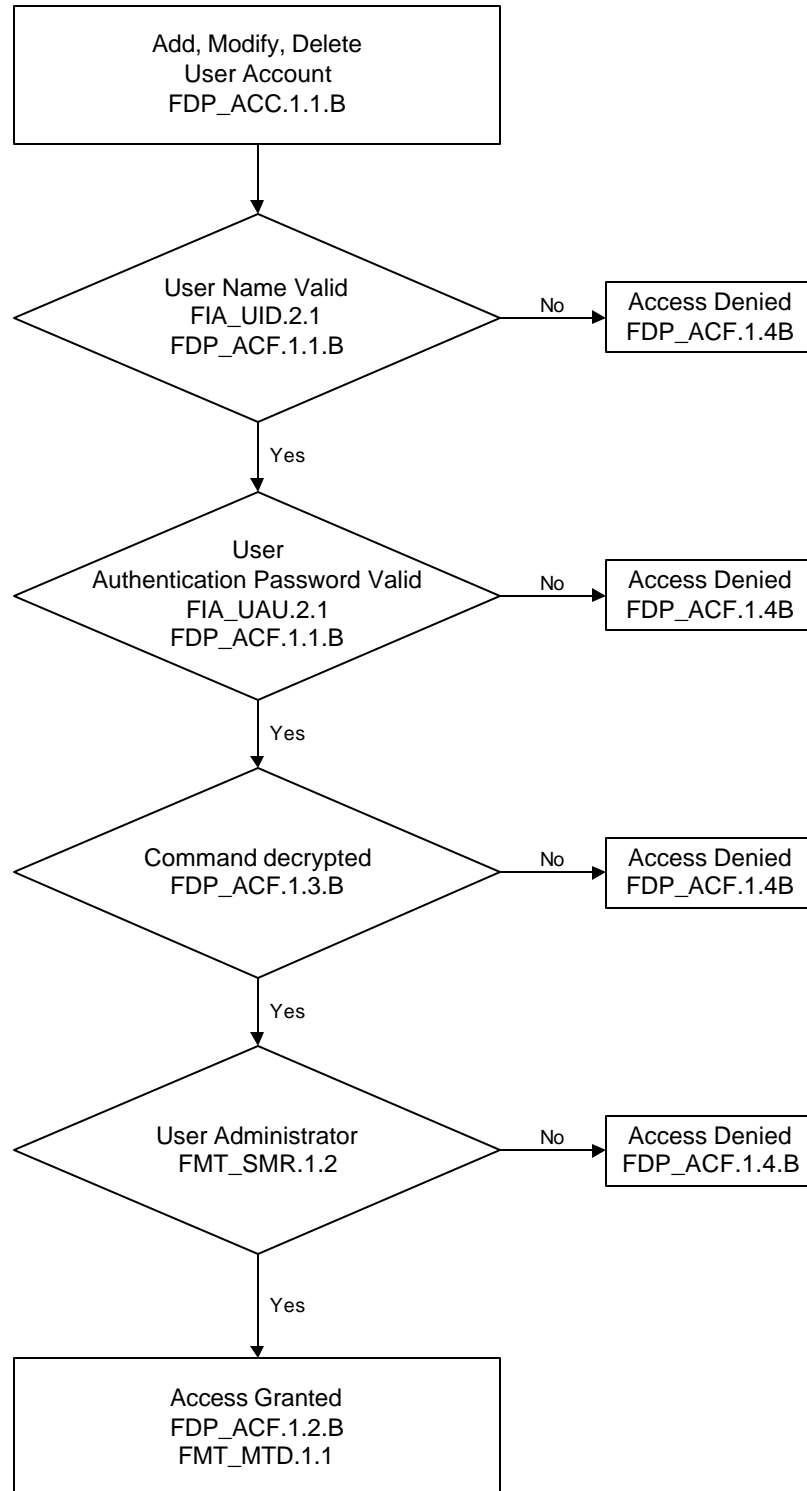
##### Crypto-Maintain

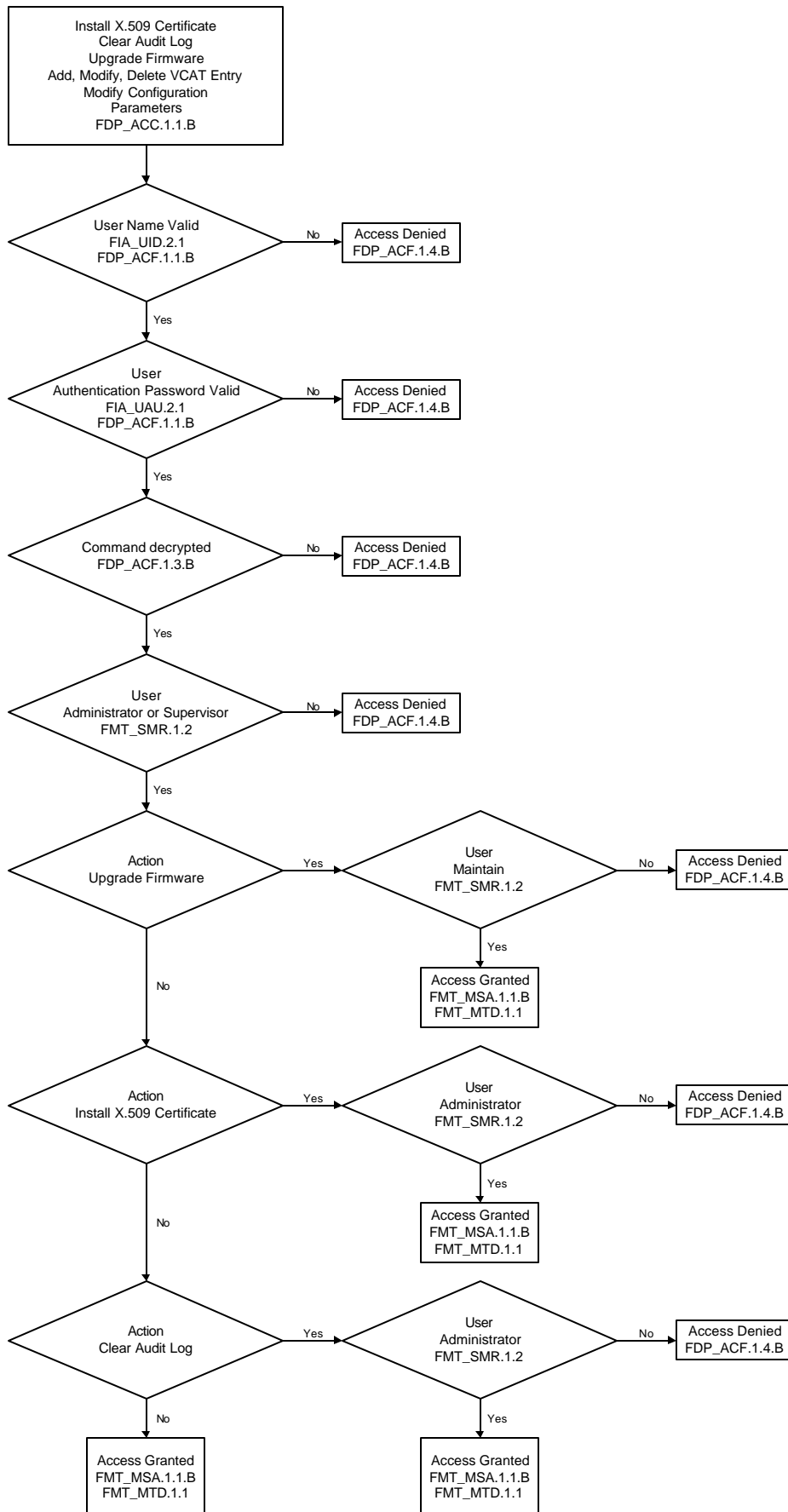
- View all configuration parameters
- View audit log
- View status
- Install firmware upgrades

Access to the internal configuration parameters is determined by the following rule.

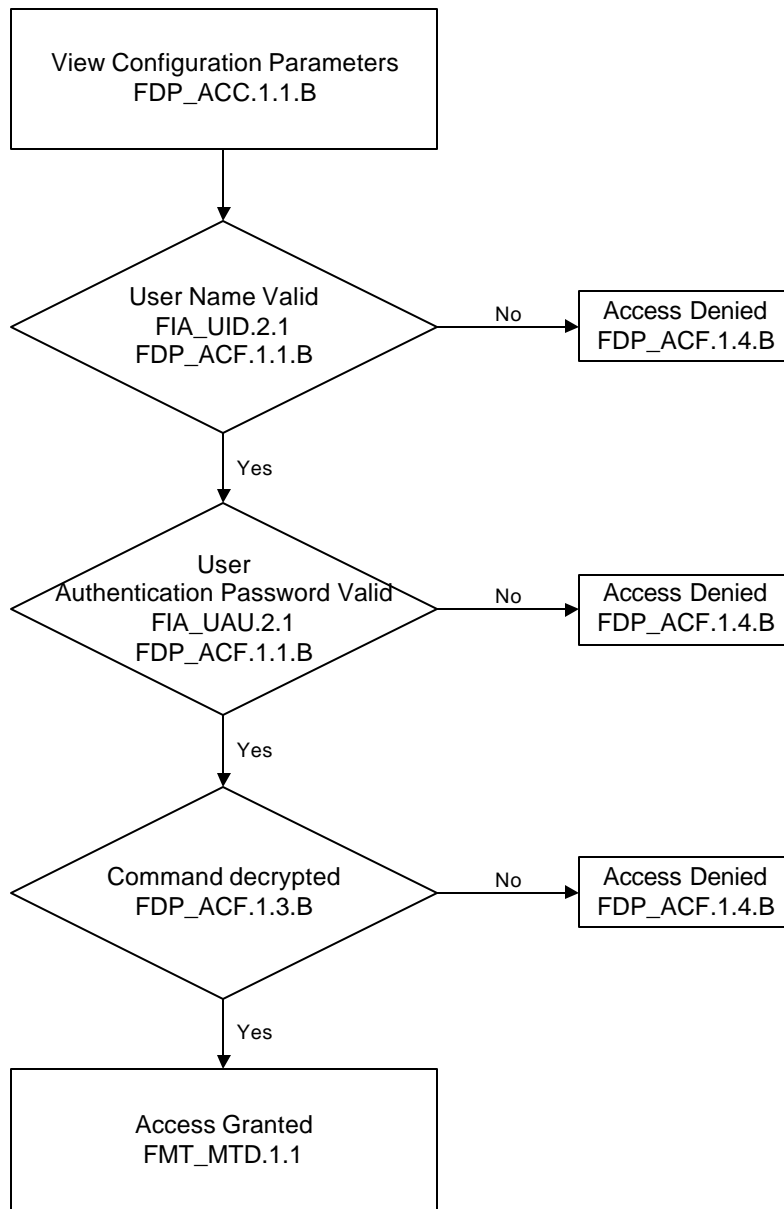
If the user name **AND** user authentication password is listed in the UAT table **AND** the user account status is active **AND** the SNMPv3 command can be decrypted then access is allowed as specified by the role otherwise access is denied.

The following diagrams demonstrate the relationship of Remote Management TOE Security Policy (TSP) model.









As shown above the remote management access control SFP traces to the following TSF functions which are, FIA\_UID.2, FIA\_UAU.2, FMT\_SMR.1, FMT\_MSA.1.1.B, FDP\_ACC.1.1.B and FDP\_ACF.1.1.B, FDP\_ACF.1.2.B, FDP\_ACF.1.3.B FDP\_ACF.1.4.B and FMT\_MTD.1.1

These are mapped to the remote user interface of the module. At this interface it accepts a username, an authentication password and an encrypted SNMPv3 command and associates a user with a role.

## 4.2 Local Management Access Security Policy

The Local Management Access SP is used to protect the User Account Table (UAT), the Virtual Channel Action Table (VCAT) and other configuration parameters from unauthorized modification.

### 4.2.1 Identification and Authentication Policies

The UAT table contains a list of operator accounts. Operators listed in the User Account Table (UAT) have access to the internal configuration parameters in the encryptor. Operators are identified by a unique user name. Authentication for each operator is achieved by the use of an authentication password.

For local access via the local console port the user name and authentication password are used as specified in RFC2274. These are the same security mechanisms used for remote access using SNMPv3.

For each operator the following security information is specified:

- User name
  - User authentication password
  - User privacy password
  - User role
  - Account Active/Inactive
- Note: Access is denied if the account is inactive.

### 4.2.2 Identity Based Access Control

The roles that can be assigned to an operator who has local management access privilege are Crypto-officer Administrator, Crypto-officer Supervisor, Crypto-officer Operator or Crypto-Maintain.

All roles can view the UAT (except for user passwords) and VCAT tables and configuration parameters.

Actions that can be performed by each role are:

#### Crypto-officer Administrators

- View all configuration parameters
- View audit log
- View status
- Add, modify and delete entries to the UAT table
- Add, modify and delete entries to the VCAT table
- Clear the audit log
- Modify configuration parameters
- Install firmware upgrades

#### Crypto-officer Supervisors

- View all configuration parameters
- View audit log
- View status
- Add, modify and delete entries to the VCAT table
- Modify configuration parameters

#### Crypto-officer Operators

- View all configuration parameters
- View audit log
- View status

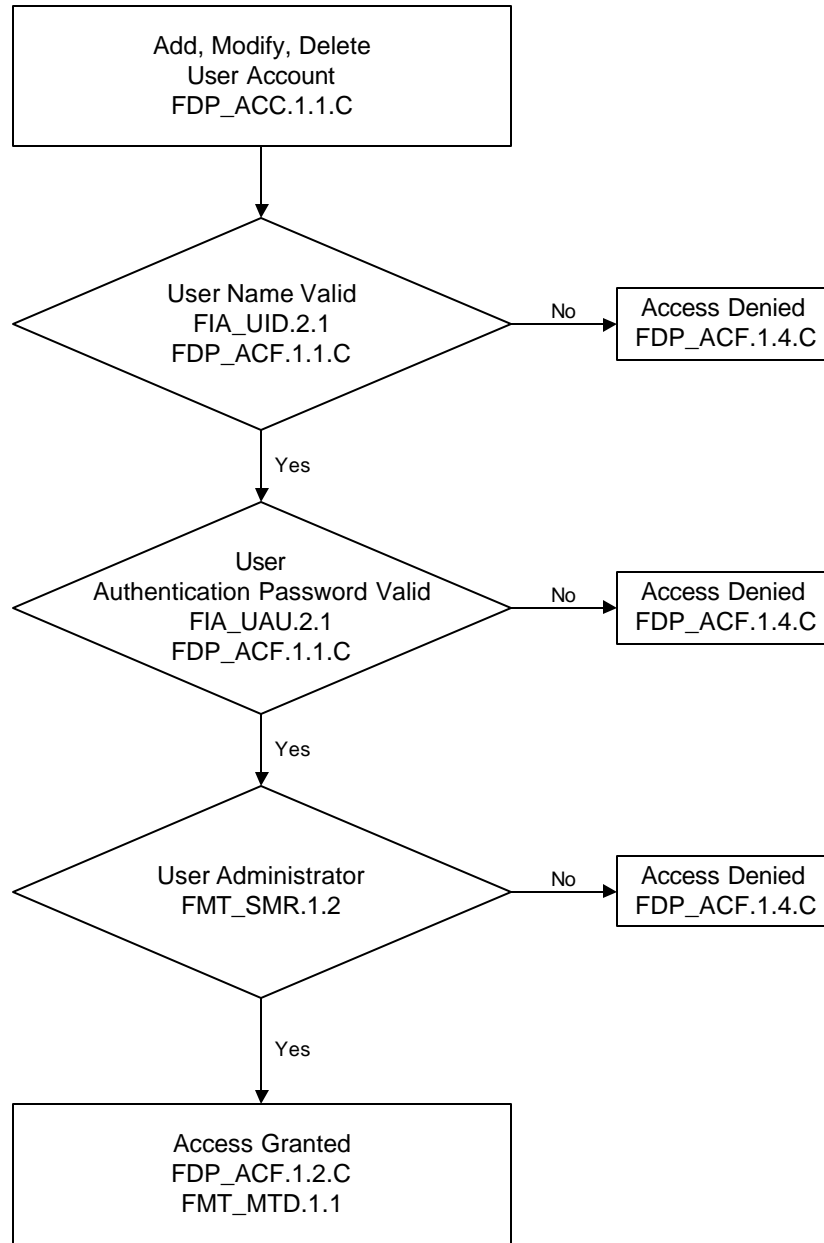
#### Crypto-Maintain

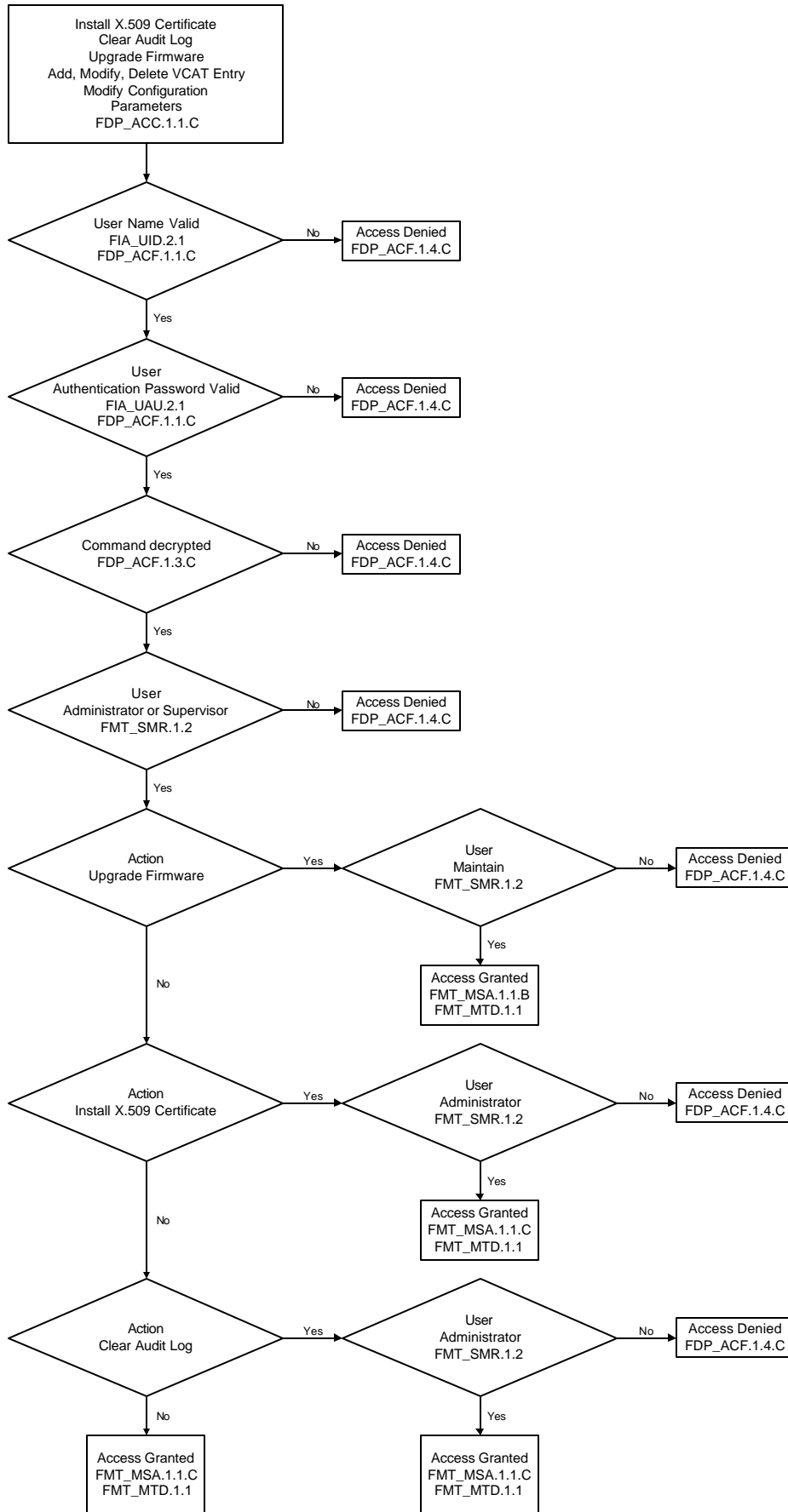
- View all configuration parameters
- View audit log
- View status
- Install firmware upgrades

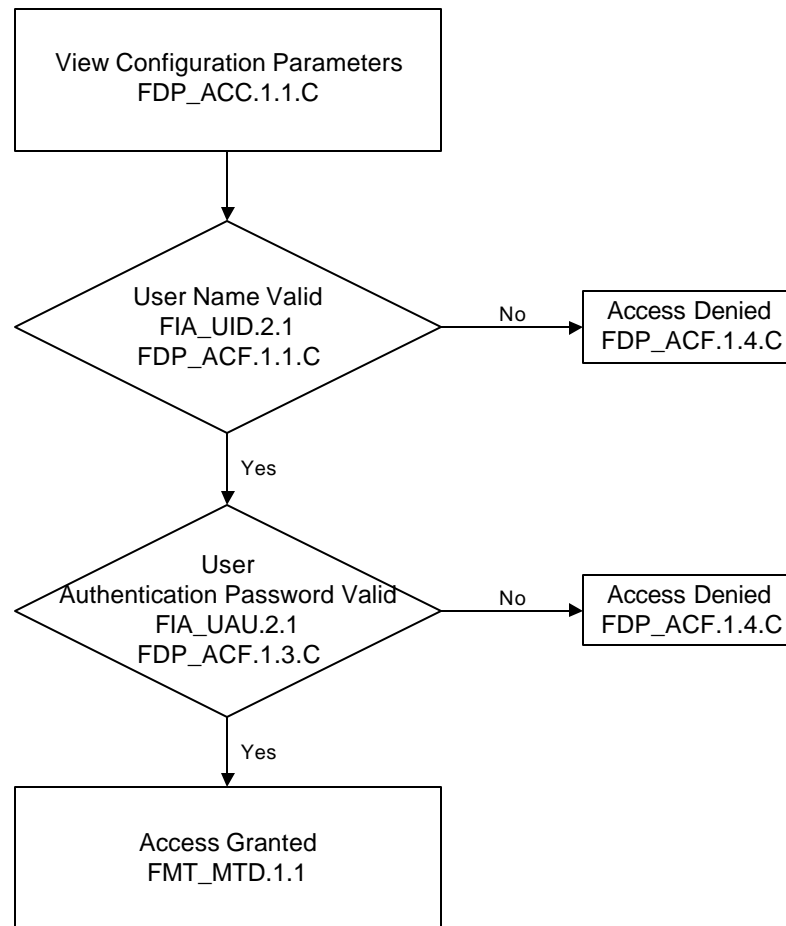
Access to the internal configuration parameters is determined by the following rule.

If the user name **AND** user authentication password is listed in the UAT table **AND** the user account status is active then access is allowed as specified by the role otherwise access is denied.

The following diagrams demonstrate the relationship of the Local Management TOE Security Policy (TSP) model.







As shown above the remote management access control SFP traces to the following TSF functions which are, FIA\_UID.2, FIA\_UAU.2, FMT\_SMR.1, FMT\_MSA.1.1.C, FDP\_ACC.1.1.C, FDP\_ACF.1.1.C, FDP\_ACF.1.2.C, FDP\_ACF.1.3.C FDP\_ACF.1.4.C, FMT\_MTD.1.1

These are mapped to the local operator interface of the module. At this interface it accepts a username and authentication password and associates a operator with a role.

### 4.3 Configuration Role

The configuration role provides the facility to change the local and network interfaces to match the ATM networks requirements and to change the power entry module to match the required input voltage. A list of the interface and power supply configurations is listed at the beginning of the Security Policy. These configurations do not affect any of the FIPS relevant functions and therefore does not affect the FIPS 140-1 validation. This role does not have any access rights to any Management Information Block (MIB) variable. Access to the unit results in automatic and immediate erase of all plain text key material and user passwords.

The operator changes the physical local and network interface modules to match the physical ATM network configuration and the power supply module to match the required power input requirements.

After changing the internal modules the operator secures the unit by placing a new tamperproof seal on the unit as described in section 2.2.

The configuration role is undertaken before the module is delivered to the end-user.

Actions that can be performed by the crypto-officer configure role are:

#### Crypto-officer Configure

- Select local interface as OC3 single mode, OC3 multimode, T3, E3, E1 or T1
- Select network interface as OC3 single mode, OC3 multimode, T3, E3, E1 or T1
- Select 110-240VAC power

- Select 24-48VDC power

#### 4.4 User Role

There is only one user role, which is another encryptor that wishes to communicate securely with the module.

Actions that can be requested by the User Role are:

##### User

- Request secure connection with encryptor.

### 4.5 Network User Services

The VCAT table contains a list of VPI/VCI addresses and the action to take when a cell with that address is received on the protected or unprotected interface ports. Only operators with the role of Crypto-officer administrator or Crypto-officer supervisor can add, modify or delete VCAT entries.

The initial state of the VCAT table has no entries hence all cells are discarded.

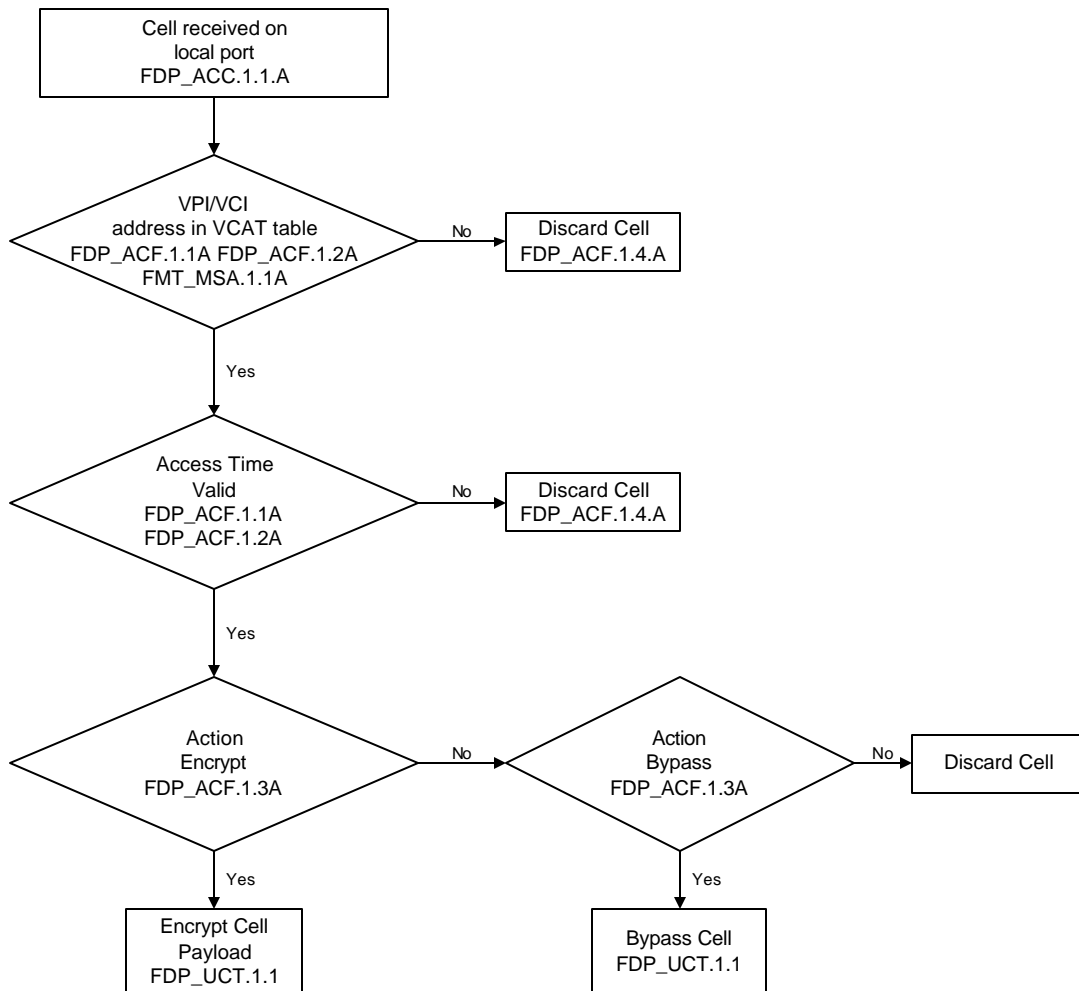
There are three possible actions for a received cell, which are:

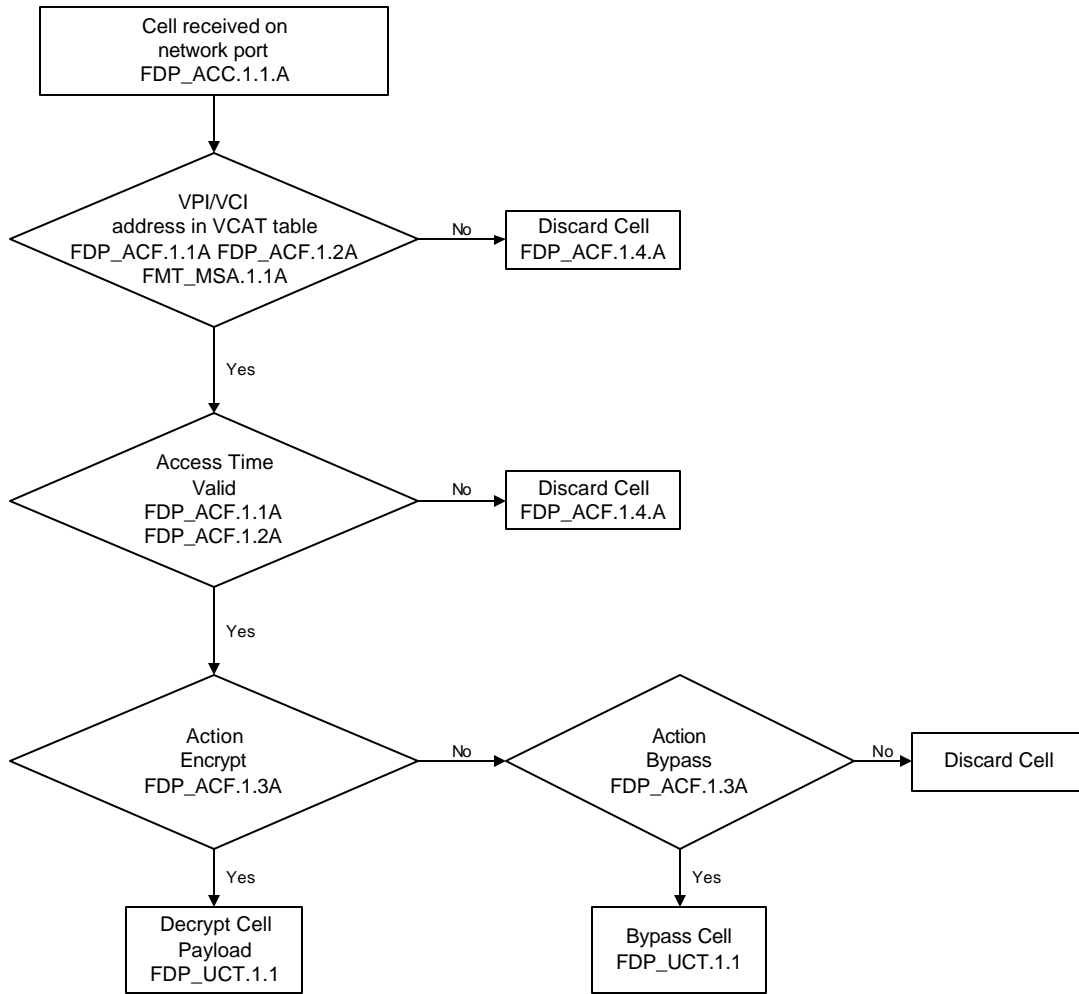
- **Encrypt/Decrypt**      The cell is encrypted if received on the protected interface port, and decrypted if received on the unprotected interface port.
- **Bypass**                      The cell is passed though the encryptor without any modification of the payload
- **Discard**                      Received cells are discarded.

The action to take for each received cell is determined by two rules. These rules are:

- **VPI/VCI Address**              Implement the action specified for this VPI/VCI address
- **Access Time**                      Discard the cell if it is received outside the specified access time for this VPI/VCI address

The following diagrams demonstrate the relationship of VCAT Based Access Control module Security Functional Requirements.





As shown above the Cell Control SFP traces to the following TSF functions, which are FDP\_ACC.1.1A, FDP\_ACF.1.1.A, FDP\_ACF.1.2.A, FDP\_ACF.1.3.A, FDP\_ACF.1.4.A and FDP\_UCT.1.1 and are mapped to the local and network interface of the module. At these interfaces cells are processed as required by the functional requirements.



## 4.6 Security Policy Enforcing Function Summary

The following security policy enforcing functions in the module implement the required functionality to enforce the Security Policy as described in section 4.

### FIA\_UID.2 User identification before any action

FIA\_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF mediated actions on behalf of that user.

### FIA\_UAU.2 User authentication before any action

FIA\_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF mediated actions on behalf of that user.

### FMT\_SMR.1 Security Roles

FMT\_SMR.1.2 The TSF shall be able to associate operators with roles.

### FDP\_ACC.1 Subset Access Control

FDP\_ACC.1.1.A The TSF shall enforce the *cell control SFP* on ATM cells received on the interfaces.

FDP\_ACC.1.1.B The TSF shall enforce the *Remote Management Access Control SFP* on all encrypted SNMPv3 packets received on the CypherCell Ethernet management port interface.

FDP\_ACC.1.1.C The TSF shall enforce the *Local Management Access Control SFP* on all data received on the CypherCell console port interface.

### FDP\_ACF.1 Security attribute based access control

FDP\_ACF.1.1.A The TSF shall enforce the *cell control SFP* to objects based on the VPI/VCI address contained in the cell header and time of day.

FDP\_ACF.1.1.B The TSF shall enforce the *Remote Management Access Control SFP* to objects based on the user ID field of the SNMPv3 packet and the user's local authentication password.

FDP\_ACF.1.1.C The TSF shall enforce the *Local Management Access Control SFP* to objects based on the user's ID and the user's local authentication password.

FDP\_ACF.1.2.A The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- *If the VPI/VCI address in the cell header is listed in the VCAT then the defined operation in the VCAT is allowed*
- *If the VPI/VCI address in the cell header is listed in the VCAT and the cell is received within the defined access times in the VCAT then the defined operation is allowed.*

FDP\_ACF.1.2.B The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- *If the User ID field in the encrypted SNMPv3 packet is listed in the User Table and the local authentication password is correct then the management operation is allowed subject to the operators defined role.*

FDP\_ACF.1.2.C The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- *If the User ID received on the console port interface is listed in the User Table and the local authenticated password is correct then console mode logon is allowed.*

FDP\_ACF.1.3.A The TSF shall explicitly authorise access of subjects to objects based on the following rules:

- *If the cell is received within the access times defined in the VCAT then the operation defined for that cell will be performed.*
- *If the operation in the VCAT is defined as "encrypt" then the cell will be passed with the cell payload encrypted/decrypted.*
- *If the operation in the VCAT is defined as "bypass" then the cell will be passed without modification.*
- *If the operation in the VCAT is defined as "discard" then the cell will be discarded without further action.*

FDP\_ACF.1.3.B The TSF shall explicitly authorise access of subjects to objects based on the following rules:

- *If the encrypted SNMPv3 packet can be decrypted and the management data is authentic then the management operation is allowed but subject to the operators defined role.*

FDP\_ACF.1.3.C The TSF shall explicitly authorise access of subjects to objects based on the following rules:

- *If the user ID presented on the console interface is listed in the user table, and the user's authentication password presented on the console interface is*

*correct then a local management session is started, allowing access to the security management functions, based on the operators defined role. Certificate Loading is never permitted from the console interface.*

- FDP\_ACF.1.4.A The TSF shall explicitly deny access of subjects to objects based on the following rules:
- *If the VPI/VCI address in the cell header is not listed in the VCAT then the cell will be discarded.*
  - *If the VPI/VCI address in the cell header is listed in the VCAT but the cell is not received within the access times defined in the VCAT then the cell will be discarded.*
- FDP\_ACF.1.4.B The TSF shall explicitly deny access of subjects to objects based on the following rules:
- *If the user ID field of the SNMPv3 packet is not listed in the user table then the management data is discarded.*
  - *If the user ID field of the SNMPv3 packet is listed in the user table and the data cannot be decrypted, then the management data is discarded.*
  - *If the user ID field of the SNMPv3 packet is listed in the user table and the data can be decrypted, but the authentication check fails then the management data is discarded.*
  - *If the user ID field of the SNMPv3 packet is listed in the user table, the data can be decrypted and the authentication check passes, but the user role is invalid then the management data is discarded.*
- FDP\_ACF.1.4.C The TSF shall explicitly deny access of subjects to objects based on the following rules:
- *If the user ID received on the console port interface is not listed in the user table then access to the management functions of the module is denied.*
  - *If the user ID received on the console port is listed in the user table and local authentication password is incorrect then access to the management function requested of the module is denied.*
  - *If the user ID received on the console port is listed in the user table and local authentication password is correct but the user role is invalid then access to the management function requested of the module is denied.*

#### **FDP\_UCT.1 Inter-TSF User Data Confidentiality Transfer Protection**

- FDP\_UCT.1.1 The TSF shall enforce the *Cell Control SFP* to be able to *transmit and receive* objects in a manner protected from unauthorised disclosure.

#### **FMT\_MSA.1 Management of security functions behavior**

- FMT\_MSA.1.1.A The TSF shall enforce the *Cell Control SFP* to restrict the ability to encrypt, bypass, or discard the ATM cells received at the module interface to those cells whose VPI/VCI address is listed in the VCAT.
- FMT\_MSA.1.1.B The TSF shall enforce the *Remote Management Access Control SFP* to restrict the ability to:
- *change\_default, modify or delete the entries in the VCAT table to Crypto-officer administrator and Crypto-officer supervisor*
  - *add, delete, or modify user accounts to Crypto-officer administrators*
  - *upgrade the modules firmware to Crypto- Maintain*
  - *activate the X.509 certificates to Crypto-officer administrators.*
- FMT\_MSA.1.1.C The TSF shall enforce the *Locale Management Access Control SFP* to restrict the ability to:
- *change\_default, modify, or delete the entries in the VCAT table to Crypto-officer administrator and Crypto-officer supervisor*
  - *add, delete, or modify user accounts to Crypto-officer administrators*
  - *upgrade the modules firmware to Crypto- Maintain*

#### **FMT\_MTD.1 Management of TSF data**

- FMT\_MTD.1.1 The TSF shall restrict the ability to
- *change\_default, query, modify, delete and clear the VCAT table, User Account table, X.509 certificate activation to Crypto-officer administrators*
  - *change\_default, query, modify, delete and clear the VCAT table and query the User Account table to Crypto-officer supervisors*
  - *query the VCAT and User Account tables to Crypto-officer operators*
  - *clear the audit log to Crypto-officer administrators*
  - *set the system time to Crypto-officer administrators and Crypto-officer supervisors*
  - *upgrade the modules firmware to Crypto- Maintain*

## 5. Physical Security Policy

CypherCell has been designed to satisfy FIPS PUB 140-1 Level 2 physical security requirements. CypherCell is housed in an opaque steel housing with external connections to the protected and unprotected network, management connections and the LCD display and keypad. The keypad ENT key can be disabled, which disables all keypad input functionality.

A tamper proof seal is provided between the removable top cover and the base. Removing the cover will destroy the seal and also activate tamper micro switches. When the micro switches are activated internal private DES keys are automatically erased irrespective of whether the unit is powered-on or powered-off.

The Crypto-Officer Administrator should regularly check that the tamper proof seal is intact. If broken the encryptor should be returned to CTAM to ensure that the encryptors internal configuration has not been tampered with.

## 6. Initialisation Policy

The following installation proceed must be followed in order to ensure the secure configuration the encryptor.

CypherManager provides a GUI to enable operators to remotely set or modify security parameters. Only CypherManager screens that have an impact on the security of the encryptor are described in this section.

CypherManager, using SNMPv3 commands, provides access to the following security parameters in CypherCell encryptors.

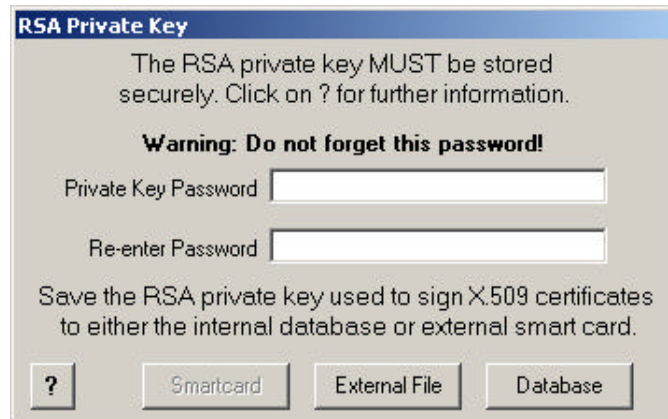
1. Installation of signed X.509 certificates
2. Creation, modification or deletion of Operators.  
Each operator when created is assigned a operator name, operator passwords and a role. Roles are Crypto-officer administrator, Crypto-officer supervisor, Crypto-officer operator and Crypto-maintain.
3. Creation, modification or deletion of VCAT entries.  
A VCAT entry specifies:
  - VPI address
  - VCI address
  - Action – Encrypt, Bypass or Discard
  - Mode – CFB or Counter, Single or Triple Two/Three key mode
  - Session key update parameters
  - Allowed access time
4. Audit Trail analysis and review. Crypto-officer administrators can also clear the audit trail.

The GUI security interfaces presented to operators are as follows:

When CypherManager is started the operator is presented with a log on screen. Operators are required to enter their user name, authentication password and privacy password if enabled. CypherManager does not store operator passwords. They are used to authenticate and encrypt the SNMPv3 commands.

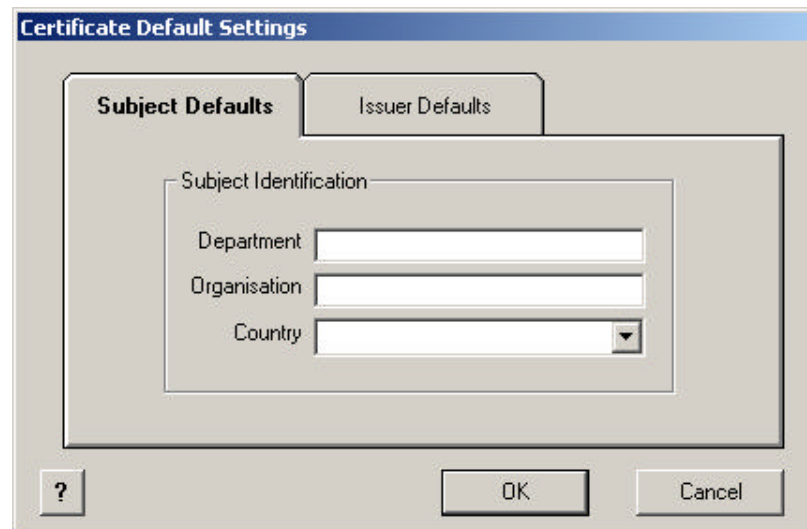


If CypherManager is being run for the first time and it has been selected as the CA, it will generate a private and public RSA key that will be used to sign X.509 certificates. The RSA keys are stored in an internal database or external file. Before the private key is stored it is encrypted using a password that has been entered by the administrator. The following screen allows the Crypto-officer administrator to enter the password, which must be at least 8 characters in length.



The RSA Private Key dialog box has a blue title bar with the text "RSA Private Key". Below the title bar, the text reads: "The RSA private key MUST be stored securely. Click on ? for further information." Below this is a warning: "Warning: Do not forget this password!". There are two text input fields: "Private Key Password" and "Re-enter Password". Below the input fields, the text reads: "Save the RSA private key used to sign X.509 certificates to either the internal database or external smart card." At the bottom, there are four buttons: "?", "Smartcard", "External File", and "Database".

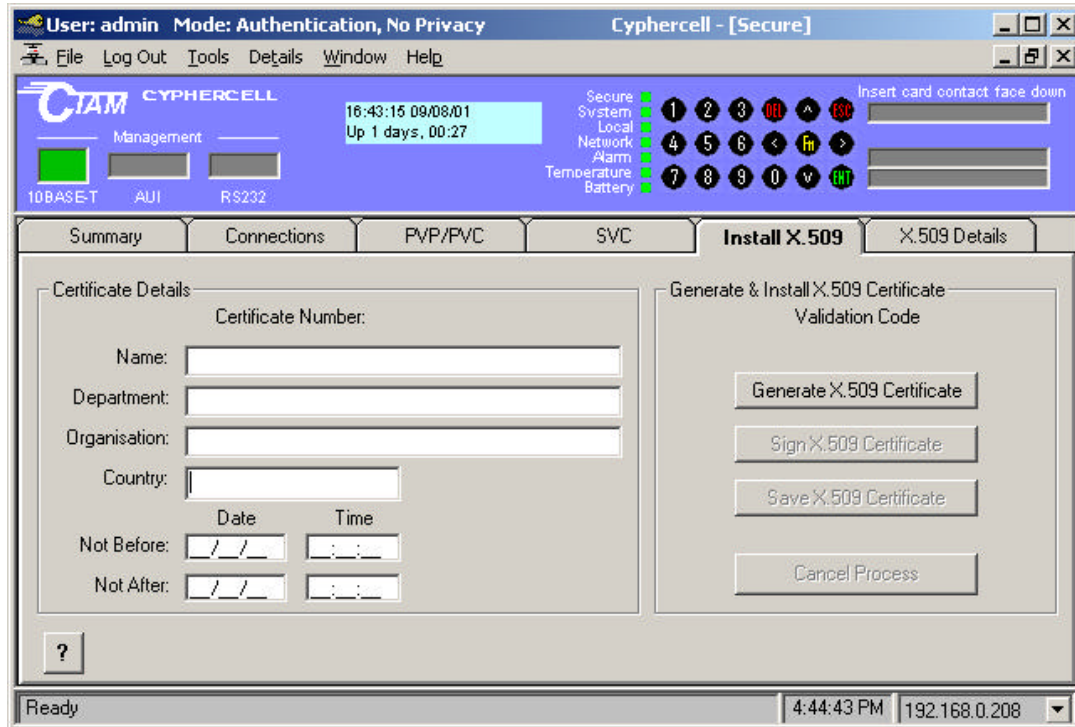
The Certificate default settings screen allows the Crypto-officer administrator to set default department, organisation and country values for the issuer and subject fields that will appear in the X.509 certificate. These values are stored in the internal database.



The Certificate Default Settings dialog box has a blue title bar with the text "Certificate Default Settings". It features two tabs: "Subject Defaults" (selected) and "Issuer Defaults". Under the "Subject Defaults" tab, there is a "Subject Identification" section containing three input fields: "Department", "Organisation", and "Country" (a dropdown menu). At the bottom, there are three buttons: "?", "OK", and "Cancel".

The next screen is used to install X.509 certificates into the encryptors. Only Crypto-officer administrators can request an unsigned X.509 certificate, sign it and then load it into the remote encryptor.

Note: The initial X.509 certificate must be loaded into the encryptor using a direct connection from the management station that is running CypherManager. The Crypto-officer administrator must ensure that no other connections can be made to the encryptor by any other device during the certificate loading process.



X.509 certificates can only be loaded into an encryptor that is set to Certificate Mode. Refer to section 2.2.3 for further details.

The process to install a X.509 certificate is as follows.

The administrator clicks the **Generate X.509 Certificate** button. The encryptor will return its public key and name. The information returned is hashed using SHA-1 and the hash value is displayed as the validation code.

After verification of the validation code the Crypto-officer administrator clicks the **Sign X.509 Certificate** button. The following screen is then displayed.



The Crypto-officer administrator must enter the private key password and Crypto-officer administrator account details. CypherManager prompts the user to re-enter the authentication and privacy passwords for verification.

Each time a new X.509 certificate is installed into an encryptor a new Crypto-officer administrator account is created if the user name is different from the existing administrator account. If the user name exists the authentication and privacy passwords will be updated with the new values. Note: If the Crypto-officer

administrator account is the default Crypto-officer administrator account (that is a valid X.509 certificate has not been loaded in the encryptor) it is always deleted and replaced by the new account.

After the Crypto-officer administrator clicks the **OK** button CypherManager signs the X.509 certificate and sends it to the remote encryptor. The contents of the certificate are hashed and the hash value is displayed as the validation code. The X.509 certificate can also be saved in an internal database by clicking the **Save X.509 Certificate** button.

The 'User Account Information' dialog box contains the following sections:

- User Details:**
  - User Name: [text box]
  - Full Name: [text box]
  - Authentication Password: [text box]
  - Privacy Password: [text box]
  - User Account Status:  Active  Inactive
- Privilege Level:**
  - Administrator  Supervisor  Operator  Maintenance
- Access:**
  - Console  SNMP

Buttons at the bottom: [?], [Apply], [Cancel]

After an X.509 certificate has been installed the Crypto-officer administrator can create supervisor and operator accounts.

Crypto-officer administrators and supervisors can also configure the VCAT table. For each defined PVP or PVC the VPI/VCI address must be entered together with the required operating mode and session key update parameters.

The 'Virtual Channel ActionTable Information' dialog box contains the following sections:

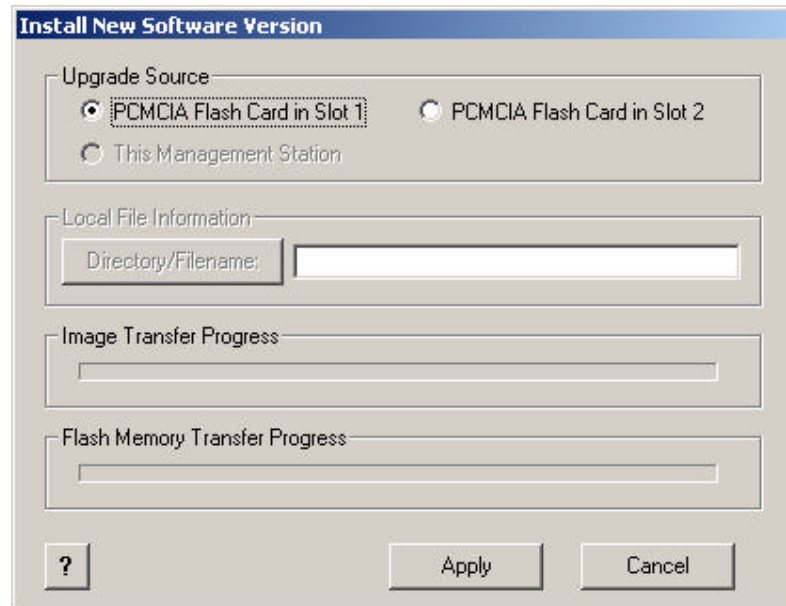
- Connection:**
  - PVP  PVC  SVC
  - Egress VPI: [text box] Egress VCI: [text box] Ingress VPI: [text box] Ingress VCI: [text box]
  - Calling NSAP Number: [text box] Called NSAP Number: [text box]
  - Connection Role:  Auto  Initiator  Responder
  - Copy
- Action:**
  - Secure  Bypass  Discard
- Encryption Mode:**
  - DES  AES
  - Single DES  2 key Triple DES  3 key Triple DES
  - CFB  CBC  Counter
- Counter Resynch Options:**
  - AAL1  Periodic  AAL3/4  AAL5
  - 500 ms
- Session Key Update:**
  - Time: hh:mm [00:00] Days: [0] Count: [0]
- Access Time:**
  - [00:00] to [00:00]
  - S M T W T F S
  -
- VCI 0 to 31 Action - Check to select bypass:**
  - 0 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
  - Buttons: [Defaults] [Select All] [Clear All]

Buttons at the bottom: [?], [Apply], [Cancel]

## 7. Firmware Upgrade Policy

CypherCell has been designed to allow the firmware to be upgraded in the field. The upgrade firmware is shipped in a PCMCIA flash memory card, which has been digitally signed by CTAM using the RSA digital signature. During the upgrade process the encryptor authenticates the new firmware using CTAM's public key before it is loaded. If the authentication fails the upgrade process is terminated.

The encryptor firmware can only be upgraded when the encryptor is placed in upgrade mode, which is selected from the front panel. Only a user who has the role of Crypto-Maintain can perform the upgrade. The upgrade command can be issued from the console port or remotely from the following screen in CypherManager.



## 8. Cryptography

### 8.1 Cryptographic Algorithms

CypherCell uses the following cryptographic algorithms and modes of operation.

- DES and TDES encryption as specified in FIPS 46-2 and FIPS 46-3 to protect ATM cells. Cells sent over the ATM network use DES or 3DES in 64-bit Cipher Feedback (CFB) mode, as defined in FIPS 81, providing a self-synchronising security solution.
- SNMPv3 commands use SHA-1 for authentication and DES in CBC mode for privacy. Sensitive information, such as user passwords, are also encrypted using the public key of the module before being encapsulated in the SNMPv3 command.
- RSA public key cryptography is used to exchange master and sessions keys between encryptors as specified in the AF-SEC-0100.00 ATM Security Specification Version 1.0 February 1999 and to sign X.509 certificates.

### 8.2 Key Management

CypherCell encryptors exchange master and session keys for each configured virtual circuit or path using RSA public key and X.509 certificates for authentication. Master keys are used to transfer periodic session keys between encryptors. Session keys are used to encrypt the payload of the ATM cell.

During installation of CypherCell, a public and private RSA key pair, are generated. When requested by CypherManager, the encryptor will send the public key to CypherManager. CypherManager creates an X.509 certificate and signs it with its private key. The signed X.509 certificate is sent back to the encryptor. The X.509 certificate is then used to authenticate CypherCell encryptors during the key exchange process.

The initial X.509 certificate must be loaded into CypherCell using a direct connection from CypherManager to the front panel Ethernet port.

### 8.3 Key Generation

All DES and RSA key pairs, except the SNMPv3 privacy key, which is derived from the user privacy password using SHA-1, as defined in RFC2574, are generated using a FIPS approved Pseudo-Random Generator as defined in FIPS PUB 186-1. The seed is sourced from an internal hardware random noise source.

### 8.4 Private/Public Key and User Password Protection

The internally generated RSA private/public key pair and the user table, which contains a hashed value of user passwords, are encrypted using three key TDES in 64-bit CBC mode and are stored in non-volatile memory. The three DES keys are stored in battery backed SRAM. These keys are automatically erased if the cover is removed.

## 9. Self-Tests

CypherCell performs the following self-tests during the start-up process:

- Management Subsystem module firmware test
- Local Interface module firmware test
- Network Interface module firmware test
- Management Subsystem module DES test known answer test
- Management Subsystem module exponentiation test
- Management Subsystem module RSA known answer test
- Management Subsystem module SHA-1 known answer test
- Encrypt module DES & TDES known answer test
- Decrypt module DES & TDES known answer test
- Bypass mode test
- RNG Test
  - The Monobit test
  - The Poker test
  - The Runs test
  - The Long Runs test

During normal operation the continuous RNG test is executed every time a request is made to the RNG process.

During normal operation, each time a private and public key pair is generated the pair-wise consistency test is executed.

The results of start-up self-tests are written to the event log. If any of the self-test fails during start-up or during an on-demand call, the module will be automatically configured to discard all ATM cells received on the local and network interfaces. An error message is displayed in the LCD display and the System LED will be set too red.

## 10. FIPS PUB 140-1 Mode of Operation

The FIPS PUB 140-1 mode of operation is defined as a mode in which only FIPS allowed or approved security mechanisms are used. These allowed/approved mechanisms are:

- DES/3DES in 64-bit CFB mode
- DES in 64-bit CBC mode
- SHA-1
- RSA public key and digital signature

The FIPS mode is controlled by customized builds of the module firmware. In order to comply with FIPS 140-1, firmware version 2.1.0 should be loaded into the module.