Security Target for
Cyphercell
ATM Encryptor

Compliant to the Common Criteria

Version

Version 3.0	20 April 2001 Release of version 3.0.

Table Of Contents

1 INTRODUCTION

1.1 Identification

The target of evaluation is Cyphercell an ATM encryptor and CypherManager a windows based SNMPv3 remote manager. Model numbers applicable to this evaluation are:

Model Number	Description
A1111A002 Software Version 1.2.1	**CYPHERCELL 155** - ATM Encryptor OC3/STM-1 Multimode Fibre Network Interface OC3/STM-1 Multimode Fibre Local Interface DES Algorithm 155Mbps throughput 1024 virtual circuits
A1221A002 Software Version 1.2.1	**CYPHERCELL 155** - ATM Encryptor OC3/STM-1 Singlemode Fibre Network Interface OC3/STM-1 Singlemode Fibre Local Interface DES Algorithm 155Mbps throughput 1024 virtual circuits
A1121A002 Software Version 1.2.1	**CYPHERCELL 155** - ATM Encryptor OC3/STM-1 Singlemode Fibre Network Interface OC3/STM-1 Multimode Fibre Local Interface DES Algorithm 155Mbps throughput 1024 virtual circuits
A1113A002 Software Version 1.2.1	**CYPHERCELL 45** - ATM Encryptor OC3/STM-1 Multimode Fibre Network Interface OC3/STM-1 Multimode Fibre Local Interface DES Algorithm 45Mbps throughput 1024 virtual circuits
A1223A002 Software Version 1.2.1	**CYPHERCELL 45** - ATM Encryptor OC3/STM-1 Singlemode Fibre Network Interface OC3/STM-1 Singlemode Fibre Local Interface DES Algorithm 45Mbps throughput 1024 virtual circuits
A1123A002 Software Version 1.2.1	**CYPHERCELL 45** - ATM Encryptor OC3/STM-1 Multimode Fibre Network Interface OC3/STM-1 Singlemode Fibre Local Interface DES Algorithm 45Mbps throughput 1024 virtual circuits
A1333A002 Software Version 1.2.1	**CYPHERCELL 45** - ATM Encryptor T3 BNC Network Interface T3 BNC Local Interface DES Algorithm 45Mbps throughput 1024 virtual circuits
A1114A002 Software Version 1.2.1	**CYPHERCELL 34** - ATM Encryptor OC3/STM-1 Multimode Fibre Network Interface OC3/STM-1 Multimode Fibre Local Interface DES Algorithm 34Mbps throughput 1024 virtual circuits
A1224A002 Software Version 1.2.1	**CYPHERCELL 34** - ATM Encryptor OC3/STM-1 Singlemode Fibre Network Interface OC3/STM-1 Singlemode Fibre Local Interface DES Algorithm 34Mbps throughput 1024 virtual circuits

Model Number	Description
A1124A002 Software Version 1.2.1	**CYPHERCELL 34** - ATM Encryptor OC3/STM-1 Singlemode Fibre Network Interface OC3/STM-1 Multimode Fibre Local Interface DES Algorithm 34Mbps throughput 1024 virtual circuits
A1334A002 Software Version 1.2.1	**CYPHERCELL 34** - ATM Encryptor T3 BNC Network Interface T3 BNC Local Interface DES Algorithm 34Mbps throughput 1024 virtual circuits
A1444A002 Software Version 1.2.1	**CYPHERCELL 34** - ATM Encryptor E3 BNC Network Interface E3 BNC Local Interface DES Algorithm 34Mbps throughput 1024 virtual circuits
A1115A002 Software Version 1.2.1	**CYPHERCELL 25** - ATM Encryptor OC3/STM-1 Multimode Fibre Network Interface OC3/STM-1 Multimode Fibre Local Interface DES Algorithm 25Mbps throughput 1024 virtual circuits
A1225A002 Software Version 1.2.1	**CYPHERCELL 25** - ATM Encryptor OC3/STM-1 Singlemode Fibre Network Interface OC3/STM-1 Singlemode Fibre Local Interface DES Algorithm 25Mbps throughput 1024 virtual circuits
A1125A002 Software Version 1.2.1	**CYPHERCELL 25** - ATM Encryptor OC3/STM-1 Singlemode Fibre Network Interface OC3/STM-1 Multimode Fibre Local Interface DES Algorithm 25Mbps throughput 1024 virtual circuits
A1335A002 Software Version 1.2.1	**CYPHERCELL 25** - ATM Encryptor T3 BNC Network Interface T3 BNC Local Interface DES Algorithm 25Mbps throughput 1024 virtual circuits
A1445A002 Software Version 1.2.1	**CYPHERCELL 25** - ATM Encryptor E3 BNC Network Interface E3 BNC Local Interface DES Algorithm 25Mbps throughput 1024 virtual circuits
A1116A002 Software Version 1.2.1	**CYPHERCELL 8** - ATM Encryptor OC3/STM-1 Multimode Fibre Network Interface OC3/STM-1 Multimode Fibre Local Interface DES Algorithm 8Mbps throughput 1024 virtual circuits
A1226A002 Software Version 1.2.1	**CYPHERCELL 8** - ATM Encryptor OC3/STM-1 Singlemode Fibre Network Interface OC3/STM-1 Singlemode Fibre Local Interface DES Algorithm 8Mbps throughput 1024 virtual circuits

Model Number	Description
A1126A002 Software Version 1.2.1	**CYPHERCELL 8** - ATM Encryptor OC3/STM-1 Singlemode Fibre Network Interface OC3/STM-1 Multimode Fibre Local Interface DES Algorithm 8Mbps throughput 1024 virtual circuits
A1336A002 Software Version 1.2.1	**CYPHERCELL 8** - ATM Encryptor T3 BNC Network Interface T3 BNC Local Interface DES Algorithm 8Mbps throughput 1024 virtual circuits
A1446A002 Software Version 1.2.1	**CYPHERCELL 8** - ATM Encryptor E3 BNC Network Interface E3 BNC Local Interface DES Algorithm 8Mbps throughput 1024 virtual circuits
A1117A002 Software Version 1.2.1	**CYPHERCELL 2** - ATM Encryptor OC3/STM-1 Multimode Fibre Network Interface OC3/STM-1 Multimode Fibre Local Interface DES Algorithm 2Mbps throughput 1024 virtual circuits
A1227A002 Software Version 1.2.1	**CYPHERCELL 2** - ATM Encryptor OC3/STM-1 Singlemode Fibre Network Interface OC3/STM-1 Singlemode Fibre Local Interface DES Algorithm 2Mbps throughput 1024 virtual circuits
A1127A002 Software Version 1.2.1	**CYPHERCELL 2** - ATM Encryptor OC3/STM-1 Singlemode Fibre Network Interface OC3/STM-1 Multimode Fibre Local Interface DES Algorithm 2Mbps throughput 1024 virtual circuits
A1337A002 Software Version 1.2.1	**CYPHERCELL 2** - ATM Encryptor T3 BNC Network Interface T3 BNC Local Interface DES Algorithm 2Mbps throughput 1024 virtual circuits
A1447A002 Software Version 1.2.1	**CYPHERCELL 2** - ATM Encryptor E3 BNC Network Interface E3 BNC Local Interface DES Algorithm 2Mbps throughput 1024 virtual circuits
A1557A002 Software Version 1.2.1	**CYPHERCELL 2** - ATM Encryptor E1 BNC Network Interface E1 BNC Local Interface DES Algorithm 2Mbps throughput 1024 virtual circuits
A1667A002 Software Version 1.2.1	**CYPHERCELL 2** - ATM Encryptor T1 RJ45 Network Interface T1 RJ45 Local Interface DES Algorithm 2Mbps throughput 1024 virtual circuits
A1040A001 Version 1.0	Adds unlimited VPI/VCI mapping option, and a maximum of 65,536 virtual circuits
S1001A001 Version 3.2.0	CypherManager Windows 95/98/ Windows NT4.0 and Windows 2000 Remote manager for CYPHERCELL encryptors. Supports SNMPv3.

1.2 Overview

This document provides a complete and consistent statement of the security enforcing functions and mechanisms of Cyphercell and CypherManager (the Target of Evaluation). The Security Target is the baseline for a formal security evaluation under the Australian Information Security Evaluation Program (AISEP).

The Security Target details the Target of Evaluation's (TOE) security requirements and the countermeasures proposed to address the perceived threats to the assets protected by the TOE.

Cyphercell together with CypherManager are intended to meet the Common Criteria EAL4 evaluation level.

Cyphercell is a high-speed encryptor, which can secure voice, data and video information transmitted over Asynchronous Transfer Mode (" ATM") Networks at data rates up to 155 Megabits per second. It can also provide access control facilities using access rules for defined virtual circuits.

Confidentiality of the transmitted information is achieved by encrypting the payload of the ATM cell while leaving the ATM header unchanged. This enables switching of the cell through ATM networks. Operation and Maintenance ("OAM") cells and Virtual Path cells with Virtual Channel Identifier ("VCI") values of 3, 4 and 6 to 15 are not encrypted enabling ATM management functionality to be maintained.

Key management and authentication are based on RSA public key cryptography and X.509 certificates providing an automated key management system.

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.

Cyphercell can be remotely managed by using CypherManager, a SNMPv3 compliant management station using a secure management session, or locally through an RS232 console port without the CypherManager application. However, Cyphercell cannot be initialised with an X.509 certificate through the console port.

1.3 CC Conformance Claim

The TOE is Part 2 Conformant and Part 3 Conformant to the Common Criteria.

1.4 References

1. Common Criteria for Information Technology Security Evaluation. 15 November 1998
2. ATM Security Specification Version 1.0 AF-SEC-0100.00 February 1999
3. RFC2574 User-based Security Model for version 3 of the Simple Network Management Protocol The Internet Society – April 1999
4. RFC2459 Internet X.509 Public Key Infrastructure – January 1999
5. PKCS #1 v2.0 RSA Cryptography Standard, RSA Laboratories July 14, 1998

1.5 Glossary of Key Terms

ATM	Asynchronous Transfer Mode
CC	Common Criteria
CLP	Cell Loss Priority
DES	Data Encryption Standard
DSD	Defence Signals Directorate
GFC	Generic Flow Control
HEC	Header Error Check
MASTER KEY	Key used to encrypt session keys
MBPS	Megabits per second
OAM	Operation and Maintenance management cells
OSP	Organisational Security Policy
PP	Protection Profile
PTI	Payload Type Indicator
PVC	Permanent Virtual Circuit
PVP	Permanent Virtual Path
RFC	Request for Comment

RSA	Public Key Algorithm
SESSION KEY	Key used to encrypt the payload of an ATM cell
SFP	Security Functional Policy
SFR	Security Functional Requirement
SNMPv3	Simple Network Management Protocol Version 3
ST	Security Target
TOE	Target of Evaluation
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 TOE Description

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 up to 155 Megabits per second (**“Mbps”**).

Cypercell 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. The Cyphercell ATM encryptor does not perform ATM switching. An example installation of the Cyphercell encryptor is shown in Figure 3.

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 (Figure 1). Cyphercell supports single or triple DES in cipher block chaining mode, cipher feedback mode or counter mode. An ATM Cell format is shown in Figure 2.

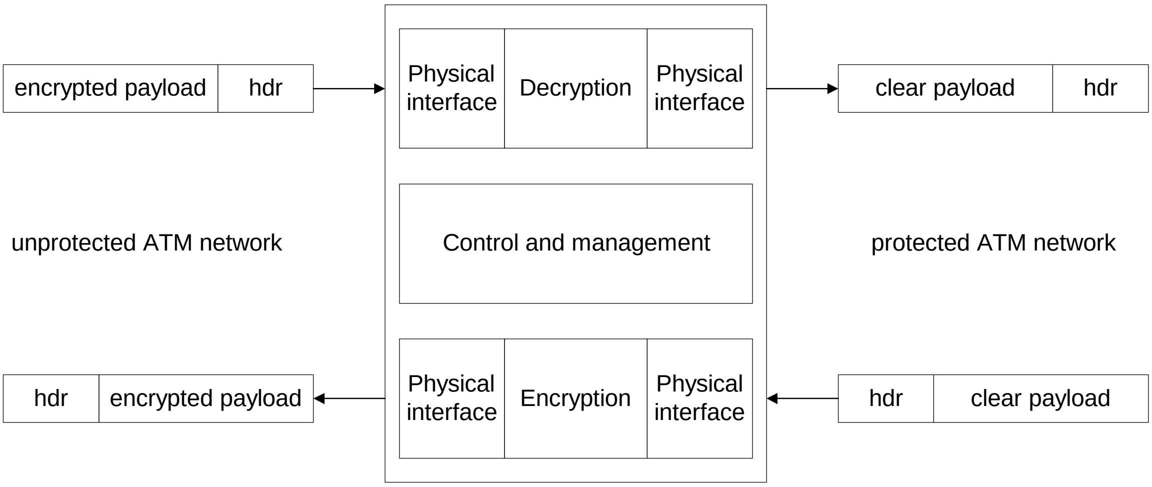

Figure 1 – CYPHERCELL Block Diagram

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 3,4 and 6 to 15 are excluded from the encryption process enabling full ATM network management functions to be maintained.

Key management and authentication are based on RSA public key cryptography and X.509 certificates providing a fully automated key management system. MASTER keys are transferred between encryptors using X.509 certificate authenticated RSA public key cryptography. SESSION keys are transferred between encryptors using MASTER keys 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 BNC coaxial connection or 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, a user 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, a user is required to present their user name and authentication password directly to the Cyphercell encryptor before a local management session is allowed. Users of the TOE cannot use the local management RS232 port to initialise the Cyphercell encryptor with an X.509 certificate. This functionality is restricted to SNMPv3 management sessions.

Cyphercell supports different types of user roles with different privileges according to a set of pre-defined roles. The three defined roles are Administrator, Supervisor and Operator. Only the Administrator has unrestricted access to the security features of the Cyphercell encryptor. Thus only the Administrator can activate X.509 certificates that are required for Cyphercell to commence operation.

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 organisation 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 Target.

3 TOE Security Environment

3.1 Assumptions

Cyphercell is intended for use in organisations that need to provide confidentiality of information transmitted over ATM networks and access control to prevent unauthorised connection to the protected ATM network. The following assumptions about the operating environment and intended use of the Cyphercell ATM encryptor and CypherManager Remote Management Station apply.

A.CERTIFICATE(operational)

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 TOE.

A.PRIVATEKEY (operational)

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

A.ENCRYPTION(operational)

Only encryption of the ATM cell payloads is required and that single DES or triple DES in cipher block chaining mode, cipher feedback mode or counter mode is appropriate for the classification of information to be protected. DSD determines the appropriateness of cryptographic mechanisms and their suitability to protect classified information.

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

Figure 2 - ATM Cell Format

A.KEYEXCHANGE (operational)

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. DSD determines the appropriateness of cryptographic mechanisms and their suitability to protect classified information.

A.AUTHENTICATE (operational)

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 (operational)

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 (operational)

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 (operational)

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 three roles:

administrator who has full access rights;
supervisor who has full access rights except they cannot add, delete or modify user accounts and they cannot install X.509 certificates; and
operator who can 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 TOE to only those authorised users who need to access those security functions.

A.MANAGEMENT (connectivity)

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

A.INSTALL (connectivity)

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. Figure 3 shows how the device could be used to secure an ATM network.

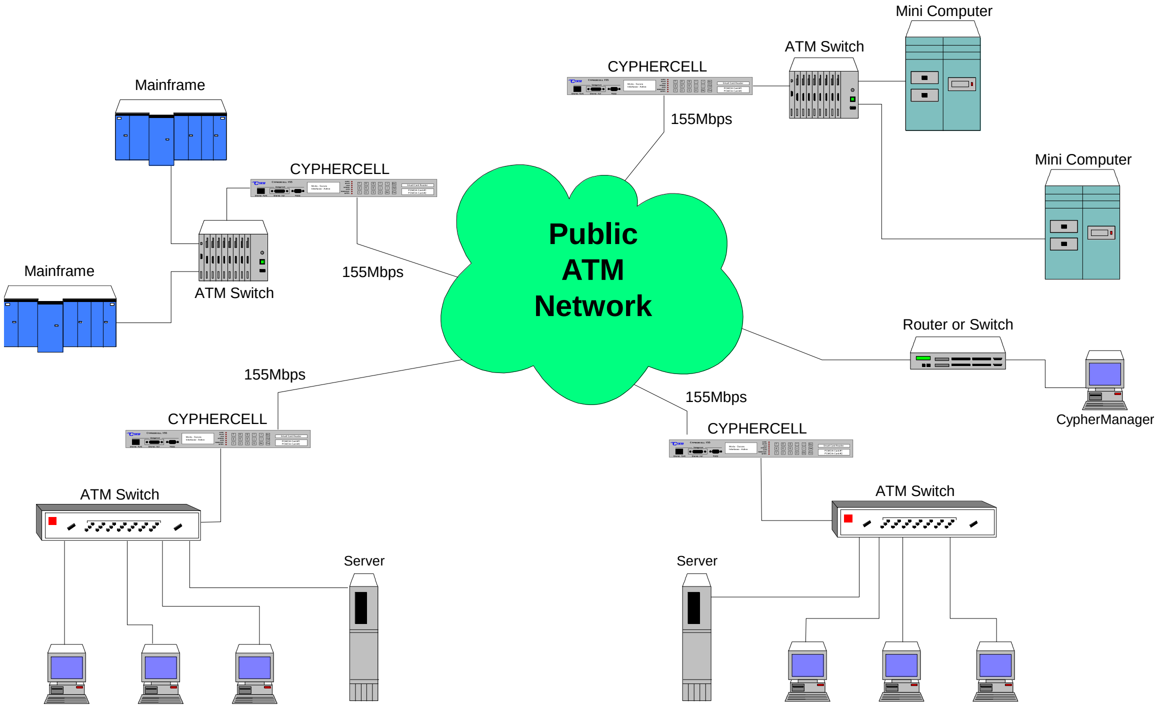

Figure 3 – A Secure ATM Network

A.REMOTEMANAGEMENT (connectivity)

It is assumed that only the CypherManager management station is used for remote management of Cyphercell. Other unevaluated SNMPv3 remote management products cannot be relied upon to provide a secure session or to format commands changing Cyphercell security parameters correctly. 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.

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 (connectivity)

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. For example, some networks protected by a firewall may implement security policies that restrict the passage of SNMPv3 packets into and out of the protected network. In this case, either SNMPv3 packets must be allowed through the firewall or the console port management function must be used.

A.PEER (connectivity)

Any other systems with which the TOE 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 TOE could not be assured.

A.LOCATE (physical)

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 (physical)

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

A.ADMIN (personnel)

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

A.ATTACKERS (personnel)

Attackers are assumed to have a high level of expertise and resources and a low level of motivation. An attacker with a high level of expertise, resources and motivation would be able to gain access to the transmitted information given a sufficient amount of time.

3.2 Threats

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

T.CAPTURE 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.

T.CONNECT An attacker (insider or outsider) may attempt to make unauthorised connections to another ATM network and transmit information, that was to be kept confidential, to another destination.

T.ABUSE An undetected compromise of information may occur as a result of an authorised user of the TOE (intentionally or otherwise) performing actions the individual is authorised to perform.

T.ATTACK 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 authorised to perform.

T.IMPERSON An attacker (outsider or insider) may impersonate an authorised user of the TOE to gain access to transmitted information that was to be kept confidential.

T.LINK 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.

T.OBSERVE An attacker could observe the legitimate use of the remote management service by an authorised user when that authorised user wishes their use of that remote management service to be kept confidential.

T.PHYSICAL Security critical parts of the TOE may be subject to physical attack which may compromise security.

T.PRIVILEGE A compromise of information may occur as a result of actions taken by careless, willfully negligent or hostile administrators or other authorised users.

3.3 Organisational Security Policies

P.CRYPTO All encryption services including, confidentiality, authentication, key generation and key management, must conform to standards specified by the Defence Signals Directorate for the protection of nationally classified information up to and including RESTRICTED and all levels of nationally sensitive classified information.

P.FILTER 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 authorised 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 C*ell Control SFP* enforced by the TOE as defined in ADV_SPM.1 (Informal TOE security policy model). The P.FILTER OSP ensures that the correct protective action is applied to any given ATM cell received by the TOE.

P.ROLES Administration of the TOE is controlled through the definition of roles, which assign different privilege levels to different types of authorised users (administrators, supervisors, and operators). This Organisational Security Policy must conform to the *Remote Management Access Control SFP* and the *Local Management Access Control SFP* enforced by the TOE as defined in ADV_SPM.1 (Informal TOE security policy model). The P.ROLES OSP ensures that administration of the TOE is performed in accordance with the concept of *least privilege*.

4 Security Objectives

4.1 TOE Security Objectives

O.ADMIN The TOE must provide functionality which enables an authorised user to effectively manage the TOE and its security functions, and must ensure that only authorised users are able to access such functionality, while also maintaining confidentiality of sensitive management data.

O.AUDIT The TOE must provide a means of recording any security relevant events, so as to assist an authorised user in the detection of potential attacks or misconfiguration of the TOE security features that would leave the TOE susceptible to attack, and also to hold users accountable for any actions that they perform that are relevant to security.

O.FILTER The TOE must provide authorised users with the means of controlling traffic flow, on the basis of ATM header information, in accordance with the set of rules defined in the P.FILTER security policy.

O.ENCRYPT The TOE must provide the means of protecting the confidentiality of information transferred across an public ATM network between two ATM switches.

O.I&A The TOE must uniquely identify all users, and must authenticate the claimed identity before granting a user access to the TOE management facilities.

O.ROLES The TOE must prevent users from gaining access to, and performing operations, on its resources for which their role is not explicitly authorised.

O.KEYMAN The TOE must provide the means for exchanging keys with only another authorised TOE.

O.CERTIFICATE The TOE must provide the means for generating signed X.509 certificates.

4.2 Environmental Security Objectives

O.AUDITLOG Authorised users of the TOE must ensure that audit facilities are used and managed effectively. In particular:

a. Appropriate action must be taken to ensure that continued audit logging, e.g. by regular archiving of logs.

b. Audit logs should be inspected on a regular basis, and appropriate action should be taken on the detection of breaches of security, or events that are likely to lead to a breach in the future.

O.AUTHDATA Those responsible for the management of the TOE must ensure that the authentication data for each account on the TOE is held securely and not disclosed to persons unauthorised to use that account.

O.CONNECT Those responsible for the TOE must ensure that no connections are provided to outside systems or users that would undermine IT security.

O.INSTALL Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which maintains IT security.

O.PHYSICAL Those responsible for the TOE must ensure that those parts of the TOE that are critical to security policy enforcement are protected from physical attack which might compromise IT security.

O.PERSONNEL Those responsible for the TOE are competent to manage the TOE and can be trusted not to deliberately abuse their privileges so as to undermine security.

5 IT Security Requirements

The TOE comprises two main components, which are *logically* connected. For ease of traceability, the Security Functional Requirements of the TOE have been defined for each component.

5.1 Cyphercell IT Security Functional Requirements

5.1.1 Identification and Authentication

- Identification of users [FIA_UID.2]
- Authentication of users [FIA_UAU.2]
- Controls over creation, deletion or modification of user accounts [FMT_MTD.1]

5.1.2 Access Control

- Role based access control [FMT_SMR.1] [FMT_MSA.1] [FMT_MSA.2] [FMT_MSA.3] [FDP_ACC.1] [FDP_ACF.1]
- VCAT based access control [FDP_ACC.1] [FDP_ACF.1] [FMT_MSA.1] [FMT_MSA.2] [FMT_MSA.3]
- Supporting SFR for Access Control time [FPT_STM.1] self test [FPT_AMT.1]

5.1.3 Audit

- Generation of Audit events [FAU_GEN.1]
- Audit trail analysis and review [FAU_SAR.1]
- Supporting SFR for Audit time [FPT_STM.1]

5.1.4 Cryptographic Key Management

- Cryptographic key generation [FCS_CKM.1]
- Cryptographic key distribution [FCS_CKM.2]
- Cryptographic key destruction [FCS_CKM.4]
- Cryptographic operations [FCS_COP.1]
- Authenticate X.509 Certificate Data for Certificate Load [FDP_DAU.1]
- Supporting SFR for CKM self test [FPT_AMT.1] tamper resistance [FPT_PHP.3]

5.1.5 Data Exchange

- Confidentiality of Transmitted Information [FDP_UCT.1] [FTP_ITC.1]
- Confidentiality of Management Data [FPT_ITT.1]

5.2 CypherManager IT Security Functional Requirements

5.2.1 X.509 Certificate Management

- Generate Signed X.509 Certificates [FCS_COP.1] [FCS_CKM.1]
- Protection of CM Private Key [FCS_COP.1]
- Authenticate X.509 Certificates & Requests [FDP_DAU.1] [FCS_COP.1]

5.2.2 Cryptographic Key Management

- Cryptographic key generation [FCS_CKM.1]
- Cryptographic operations [FCS_COP.1]

5.2.3 Data Exchange

- Confidentiality of Management Data [FPT_ITT.1]

5.3 TOE Security Assurance Requirements

Cyphercell together with CypherManager are intended to meet the Common Criteria EAL4 evaluation level.

5.4 Security Requirements on the IT Environment

In the absence of appropriate physical access controls, the private key used to sign X.509 certificates must be held in a secure environment.

6 TOE Summary Specification

6.1 TOE Security Functions

6.1.1 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.

6.1.2 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.

6.1.3 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles *administrator, supervisor and operator*.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.1.4 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*.

6.1.5 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 users 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 users 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 users 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 TOE 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 TOE 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 TOE is denied.*

6.1.6 FAU_GEN.1 Audit Data Generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions
b) All auditable events for the *minimum* level of audit and
c) *FMT_MTD.1 All modifications to the values of the TSF data*
d) *FPT_AMT.1 Execution of the tests of the underlaying machine and the results of the tests*

FAU_GEN.1.2 The TSF shall record within each audit record the following information:

a) Date and time of the event, type of event, subject identity and the outcome (success or failure) of the event and
b) For each audit event type, based on the auditable event definitions of the functional components included in the ST,

FCS_CKM.1	*Success and failure of the activity*
FCS_CKM.2	*Success and failure of the activity*
FCS_CKM.4	*Success and failure of the activity*
FCS_COP.1	*Success and failure, and the type of cryptographic operation*
FDP_ACF.1	*Successful requests to perform an operation on an object covered by the SFP*
FDP_DAU.1	*Successful generation of validity evidence*
FDP_UCT.1	*The identity of any user or subject using the data exchange mechanism*
FIA_UID.2	*Unsuccessful use of the user identification mechanism, including the user identity provided*
FIA_UAU.2	*Unsuccessful use of the user authentication mechanism*
FMT_MSA.2	*All offered and rejected values for a security attribute*
FMT_SMR.1	*Modifications to the group of users that are part of a role*
FPT_STM.1	*Changes to the time*
FTP_ITC.1	*Failure of the trusted channel functions*
	Identification of the initiator and target of failed trusted channel functions

6.1.7 FAU_SAR.1 Security Audit Review

FAU_SAR.1.1 The TSF shall provide *all authorised users* with the capability to read *all audit information* from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.1.8 FCS_CKM.1 Cryptographic Key Generation

FCS_CKM.1.1.A The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm, *hardware random noise source*, and specified cryptographic key sizes ***DES - 56 bits, 112 bits, 168 bits, RSA – 1024 bit****s* that meet the following standard: *DSD, as the National COMSEC Authority, requirements for Cryptographic Key generation*.

FCS_CKM.1.1.B The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm, *SNMPv3 key generation using user passwords*, and specified cryptographic key sizes *SNMPv3 privacy and authentication keys – 128 bits* that meets the following standard *RFC2574.*

FCS_CKM.1.1.C The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm, *(pseudo-random sequence generation)*, and specified cryptographic key sizes *RSA – 1024 bits, DES – 56 bits, 112 bits 168 bits,* that meet the following standard: *DSD, as the National COMSEC Authority, requirements for Cryptographic Key generation.*

6.1.9 FCS_CKM.2 Cryptographic Key Distribution

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method, *RSA public key and Master/Session key using X.509 certificates for authentication*, that meets the following standard: *ATM Forum Security Specification V1.0, PKCS #1*

6.1.10 FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method: *The keys used to encrypt the payload of the ATM cell are held in volatile memory. Loss of electrical power will destroy all DES keys. If the case is opened all key material is automatically erased including the RSA private key and user passwords* that meets the following standard: *DSD, as the National COMSEC Authority, requirements for Cryptographic Key Destruction.*

6.1.11 FCS_COP.1 Cryptographic Operation

FCS_COP.1.1.A The TSF shall perform *hardware 64 bit Cipher Block Chaining, 64 bit Cipher Feedback and counter mode* in accordance with a specified algorithm, *DES* and cryptographic key sizes *56 bits, 112 bits and 168 bits* that meet the following standards: *FIPS PUB 46-2 and FIPS PUB 81 and ATM Forum Security Specification V1.0*.

FCS_COP.1.1.B The TSF shall perform *public key encryption* in accordance with a specified algorithm *RSA* and cryptographic key sizes *1024 bits* that meet the following: *ATM Forum Security Specification V1.0, PKCS#1.*

FCS_COP.1.1.C The TSF shall perform *message digest generation/verification* in accordance with a specified algorithm *MD5* and cryptographic key sizes *128 bits*, that meet the following standards: *ATM Forum Security Specification V1.0, RFC2574*

FCS_COP.1.1.D The TSF shall perform *digital signature generation* in accordance with a specified algorithm *RSA public key* and cryptographic key sizes *1024 bits* that meets the following standards: *PKCS#1.*

FCS_COP.1.1.E The TSF shall perform *software 64 bit Cipher Block Chaining* in accordance with a specified algorithm, *DES* and cryptographic key sizes *56 bits, 112 bits and 168 bits* that meet the following standards: *FIPS PUB 46-2 and FIPS PUB 81.*

6.1.12 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.

6.1.13 FTP_ITC.1 Inter-TSF Trusted Channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and a remote *instance of the TOE* that is logically distinct from other communication channels and provides assured identification of its end-points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit the *TSF or the remote instance of the TOE* to initiate communication via the channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for *all cell traffic* as defined by *the Cell Control SFP*.

6.1.14 FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

6.1.15 FPT_AMT.1 Abstract machine testing

FPT_AMT.1.1 The TSF shall run a suite of self tests *during initial start-up and periodically during normal operation* to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlines the TSF.

6.1.16 FPT_PHP.3 Resistance to physical attack

FPT_PHP.3.1.A The TSF shall resist *attempts, by opening the unit, to gain physical access* to the *key material* by responding automatically such that the TSP is not violated.

FPT_PHP.3.1.B The TSF shall resist *attempts, by opening the unit, to gain physical access* to the *password data* by responding automatically such that the TSP is not violated.

6.1.17 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 TOE 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 *administrator and supervisor*
- *add, delete, or modify user accounts* to *administrators*
- *activate* the *X.509 certificates* to *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 *administrator and supervisor*
- *add, delete, or modify user accounts* to *administrators*

6.1.18 FMT_MSA.2 Secure security attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes

6.1.19 FMT_MSA.3 Static attribute initialisation

FMT_MSA.3.1.A The TSF shall enforce the *Cell Control SFP* to provide *restrictive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.1.B The TSF shall enforce the *Remote Management Access Control SFP* to provide *restrictive* default values that are used to enforce the SFP.

FMT_MSA.3.1.C The TSF shall enforce the *Local Management Access Control SFP* to provide *restrictive* default values that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the *administrator or supervisor* to specify the alternative initial values to override the default values when an object or information is created.

6.1.20 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 *administrators*
- *change_default, query, modify, delete and clear* the *VCAT table and query the User Account table* to *supervisors*
- *query* the *VCAT and User Account tables* to *operators*
- *clear the audit log* to *administrators*
- *set the system time* to *administrators* and *supervisors*

6.1.21 FDP_DAU.1 Basic Data Authentication

FDP_DAU.1.1 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of *X.509 Certificate generation requests from a Cyphercell and New X.509 Certificates generated by CypherManager for a Cyphercell.*

FPD_DAU.1.2 The TSF shall provide the *administrators* with the ability to verify evidence of the validity of the indicated information.

6.1.22 FPT_ITT.1 Basic Internal Transfer Protection

FPT_ITT.1.1 The TSF shall protect TSF data from *disclosure* when it is transmitted between physically-separated parts of the TOE.

6.2 Summary of TOE Security Functions

The TOE security functions have all been derived from the Common Criteria Part 2: Security Functional Requirements. Below is a higher level summary of the IT Security Functions based on those defined in section 6.1. This has been done to provide a summary of the TOE Security Functions without dependence upon knowledge and understanding of the Common Criteria:

F.CELLCONTROL

The TOE shall control the access of ATM cells received on the private network interface and on the public network interface on the basis of:

a. The VPI/VCI address in the ATM Cell Header; and
b. The time of day.

In doing so, the TOE shall take one of three possible actions, encrypt/decrypt the ATM cell payload (using DES in CBC, CFB or counter mode), pass the ATM cell unchanged or discard the ATM cell.
The TOE determines the appropriate action to take on any given ATM cell by examining the list of entries in the VCAT. By default, for a given VPI/VCI that is not listed in the VCAT, the ATM cell is discarded. Only Administrators and Supervisors are allowed to add, modify and delete entries within the VCAT.

This function maps to the following functions identified in section 6.1:

FDP_ACC.1.1.A FDP_ACF.1.1.A FDP_ACF.1.2.A FDP_ACF.1.3.A
FDP_ACF.1.4.A FMT_MSA.1.1.A FMT_MSA.2.1 FMT_MSA.3.1.A
FMT_MSA.3.2 FPT_STM.1.1

F.KEYMANAGEMENT

The TOE shall manage all the necessary keys to support its cryptographic operations, namely:

a. Generating and securely transferring master keys between encryptors. Master keys are distributed between encryptors using RSA public key cryptography and X.509 certificates for authentication;
b. Updating session keys used for DES encryption between encryptors using DES Master keys. DES session keys are periodically updated according to local security policy requirements set by Administrators or Supervisors. Session keys are distributed as OAM cells on an ATM network;
c. Generating privacy DES keys and authentication keys for SNMPv3 management. ;
d. Generating RSA public/private key pairs for both CypherManager and Cyphercell;
e. Protecting user passwords used for generating privacy DES keys and authentication keys, during user account setup on a Cyphercell, by encrypting the password data with the public key of the intended Cyphercell encryptor that will operate the user account.
f. Generating signed X.509 certificates; and
g. Calculating MD5 message digests.

This function maps to the following functions identified in section 6.1:

FCS_CKM.1.1.A FCS_CKM.1.1.B FCS_CKM.1.1.C
FCS_CKM.2.1 FCS_CKM.4.1
FCS_COP.1.1.B FCS_COP.1.1.C FCS_COP.1.1.D FCS_COP.1.1.E
FDP_DAU.1.1 FDP_DAU.1.2

F.IDENTIFICATION_AND_AUTHENTICATION

To modify and view any of the security attributes of the TOE for administrative purposes, authorised users must identify and authenticate via one of two mechanisms depending on whether they are using the SNMPv3 remote management functionality or the console mode management functionality. Identification and Authentication services are performed by the Cyphercell encryptor only.

For remote management using SNMPv3, the CypherManager remote management station will generate an appropriate authentication key, used to authenticate the remote management data, and a privacy key used to 56-bit DES encrypt the remote management data. Both keys are generated on the CypherManager remote management station from the SNMPv3 Engine ID of the Cyphercell encryptor, and a user password. CypherManager requires a password length of a minimum of 8 characters. The set of possible characters are A-Z, a-z, 0-9 and ` ~ ! @ # $ % ^ & * ( ) _ - + = { [}] : ; ” ’ , < . > ? / | \.

The remote management data is encrypted and associated with a user ID entered by the user on the CypherManager to make the SNMPv3 packet. The encrypted SNMPv3 packets are then sent to Cyphercell. For Cyphercell, User ID, local privacy passwords and local authentication passwords are stored within the User Account Table of the encryptor, with the first administrator account being setup during the initialisation of the Cyphercell. If Cyphercell cannot decrypt the data or the authentication process as specified in RFC2574 fails, then the identification and authentication of that SNMPv3 data fails, the SNMPv3 data is discarded, and the event is audited. Each SNMPv3 packet is identified and authenticated in this way.

For local management using the console port of the Cyphercell encryptor, users logon to the Cyphercell by supplying a user ID and their authentication password. The Cyphercell then compares the user ID and the password supplied with the local authentication password. If the authentication password does not match, for that user ID in the Cyphercell User Account Table, then identification and authentication fails, the console session is not started, and the event is audited. If the user ID and authentication password match the entry in the user table, a console session is opened. Once the session is opened the user can perform actions on the TSF, in accordance with their defined role, until the session is closed. X.509 certificate load operations cannot be performed through the console port.

This function maps to the following functions identified in section 6.1:

FIA_UID.2.1 FIA_UAU.2.1 FMT_MTD.1.1

F.ROLE_BASED_ACCESS

The TOE defines three roles for accessing the TSFs. These are:

Administrators: Who can change defaults, query, modify, delete and clear the VCAT, User accounts, activate X.509 certificates, clear the audit log, view the audit log and set the system time.

Supervisors: Who can change defaults, query, modify, delete and clear the VCAT, view the User accounts table and audit log and set the system time.

Operators: Who can query the VCAT and User Account tables only, and view the audit log.

The TOE associates users with these roles and prevents a user from performing operations on the TSF that they are not authorised to perform.

This function maps to the following functions identified in section 6.1:

FDP_ACC.1.1.B FDP_ACC.1.1.C FDP_ACF.1.1.B FDP_ACF.1.1.C
FDP_ACF.1.2.B FDP_ACF.1.2.C FDP_ACF.1.3.B FDP_ACF.1.3.C
FDP_ACF.1.4.B FDP_ACF.1.4.C FMT_SMR.1.1 FMT_SMR.1.2
FMT_MSA.1.1.B FMT_MSA.1.1.C FMT_MSA.2.1 FMT_MSA.3.1.B
FMT_MSA.3.1.C FMT_MSA.3.2 FMT_MTD.1.1

F.SNMP

The TOE shall protect the confidentiality of remote management data between the Cyphercell encryptors and the CypherManager remote management station. The TOE encrypts SNMPv3 data packets using 56-bit DES keys that are derived from the Engine ID of the Cyphercell being managed and the user’s privacy password.

This function maps to the following functions identified in section 6.1:

FCS_COP.1.1.E FPT_ITT.1.1

F.ENCRYPTION

The TOE shall provide a trusted communications channel between itself and other Cyphercell encryptors managed by the same CypherManager remote management station, to protect the confidentiality of transmitted information. The TOE encrypts ATM cells on the basis of the VPI/VCI in the ATM cell header and whether the VCAT entry requires encryption of traffic on that VPI/VCI. If encryption is required, Cyphercell performs hardware-based 56, 112 or 168 bit DES encryption in CBC, CFB or counter mode on the ATM cell payload.

This function maps to the following functions identified in section 6.1:

FCS_COP.1.1.A FDP_UCT.1.1 FTP_ITC.1.1 FTP_ITC.1.2
FTP_ITC.1.3

F.AUDIT

Audit data is generated only within the Cyphercell encryptor, and stored in an audit table within internal RAM. All auditable events are associated with operations that occur in Cyphercell only, thus there is no requirement for audit logs on the CypherManager.

The TOE is able to generate an audit record for each of the auditable events listed in FAU_GEN.1.1 and FAU_GEN.1.2.

Authorised users can view the audit log, through SNMPv3 remote management from CypherManager, or through the console port. In each case, the user is identified and authenticated before access is granted to the audit log. In each case, the data is presented in a human readable format, with CypherManager providing a GUI for audit data review, and the console mode presenting the data as a scrolled list of audit text.

The audit log has a finite size for logging audit records. Once this space has been used, the audit log is either cycled back around, or disabled as selected by the administrator. Alternatively, the Administrator is permitted to clear the audit log at any time.

This function maps to the following functions identified in section 6.1:

FAU_SAR.1.1 FAU_SAR.1.2 FAU_GEN.1.1 FAU_GEN.1.2
FPT_STM.1.1

F.SELF_PROTECT

The TOE protects itself from attempts to get access to the user passwords and key material stored within Cyphercell. A microswitch mechanism is provided that is activated whenever the case is opened. Once activated, all key material and user password data is erased from volatile RAM. Further, the Cyphercell regularly performs self-tests of internal hardware and operations to check that the underlying functionality of the TSF is functioning correctly with the results of these tests are audited.

The TOE protects its own private key on CypherManager by encrypting the private key using triple DES and a passphrase. Only a user who has access to the passphrase can unlock the private key of the CypherManager.

This function maps to the following functions identified in section 6.1:

FPT_AMT.1.1 FPT_PHP.3.1.A FPT_PHP.3.1.B FCS_COP.1.1.E

The set of high level IT security functions map directly onto functions derived from the Common Criteria Part 2 Security Functional Requirements. These CC Part 2 requirements have been used in the subsequent analyses and mapping's to demonstrate suitability and mutual support of TOE security functions. Therefore, it is possible to trace how these high level functions contribute to satisfying the TOE SFRs.

6.3 TOE IT Security Assurance Requirements

Appropriate assurance measures have been and are being employed to meet the assurance requirements for the Common Criteria EAL4 evaluation level.

7 Security Target Rationale

7.1 Security Objectives Rationale

7.1.1 Mapping of Threats, OSPs and Assumptions to Objectives

The following tables demonstrate that the each threat, OSP and assumption is addressed by at least one objective, and each objective addresses at least one threat, OSP or assumption.

Objectives ========== Assumptions, Threats, OSPs	O.ADMIN	O.AUDIT	O.FILTER	O.ENCRYPT	O.I&A	O.ROLES	O.KEYMAN
A.CERTIFICATE							
A.PRIVATEKEY	🗳						
A.ENCRYPTION				🗳			
A.KEYEXCHANGE							🗳
A.AUTHENTICATE							🗳
A.ACCESS			🗳				
A.AUDIT		🗳					
A.ROLES	🗳				🗳	🗳	
A.MANAGEMENT	🗳						
A.INSTALL							
A.REMOTE-MANAGEMENT	🗳				🗳		
A.SNMP	🗳						
A.PEER	🗳						
A.LOCATE							
A.CYPHER-MANAGER							
A.ADMIN	🗳		🗳		🗳	🗳	
A.ATTACKERS	🗳	🗳	🗳	🗳	🗳	🗳	🗳
T.CAPTURE			🗳	🗳			🗳
T.CONNECT	🗳	🗳	🗳		🗳	🗳	🗳
T.ABUSE		🗳				🗳	
T.ATTACK	🗳	🗳			🗳	🗳	
T.IMPERSON	🗳	🗳			🗳	🗳	🗳
T.LINK			🗳	🗳			🗳
T.OBSERVE				🗳			🗳
T.PHYSICAL							
T.PRIVILEGE		🗳			🗳	🗳	
P.CRYPTO				🗳			🗳
P.FILTER	🗳		🗳				
P.ROLES	🗳					🗳	

Objectives ========== Assumptions, Threats, OSPs	O.AUDITLOG	O.AUTHDATA	O.CONNECT	O.INSTALL	O.PHYS	O.CERT	O.PERS
A.CERTIFICATE						✓	
A.PRIVATEKEY					✓		✓
A.ENCRYPTION							
A.KEYEXCHANGE						✓	
A.AUTHENTICATE						✓	
A.ACCESS							
A.AUDIT	✓						
A.ROLES							
A.MANAGEMENT							
A.INSTALL				✓			
A.REMOTE-MANAGEMENT			✓	✓			
A.SNMP			✓	✓	✓		
A.PEER			✓	✓	✓		✓
A.LOCATE			✓	✓	✓		
A.CYPHER-MANAGER			✓	✓	✓		
A.ADMIN							✓
A.ATTACKERS	✓	✓	✓	✓	✓	✓	✓
T.CAPTURE			✓	✓	✓	✓	✓
T.CONNECT		✓	✓	✓	✓	✓	✓
T.ABUSE	✓	✓					✓
T.ATTACK	✓	✓	✓	✓	✓		✓
T.IMPERSON	✓	✓	✓	✓	✓	✓	✓
T.LINK						✓	
T.OBSERVE						✓	
T.PHYSICAL				✓	✓		✓
T.PRIVILEGE	✓	✓					✓
P.CRYPTO						✓	
P.FILTER							
P.ROLES							

7.1.2 Informal argument of adequacy and correctness of mapping

A.CERTIFICATE

- O.CERTIFICATE ensures that the TOE requires that a valid X.509 certificate, signed by the CypherManager Management Station, be loaded into Cyphercell before secure operation can commence.

A.PRIVATEKEY

- O.ADMIN provides the necessary functionality for authorised users to manage the security features of the TOE.
- O.PHYSICAL ensures that the protected private key of CypherManager is kept within a secure environment.
- O.PERSONNEL ensures that the users who have access to the password for the private key are trusted and competent to manage that password appropriately.

A.ENCRYPTION

- O.ENCRYPT provides the means for protecting the confidentiality of information transferred across the public ATM network.

A.KEYEXCHANGE

- O.KEYMAN and O.CERTIFICATE provide a means for exchanging keys between authorised TOEs.

A.AUTHENTICATE

- O.KEYMAN and O.CERTIFICATE ensure that X.509 certificate based authentication occurs between authorised TOEs.

A.ACCESS

- O.FILTER provides the means for controlling traffic flow on the basis of ATM header information in accordance with a set of defined rules.

A.AUDIT

- O.AUDIT and O.AUDITLOG provide a means of recording security relevant events and the facilities to effectively manage audit information.

A.ROLES

- O.ROLES allows for the definition of roles for authorised users on the basis of least privilege.
- O.ADMIN provides the facility for an authorised user to manage the TOE and its security functions.
- O.I&A and O.AUTHDATA ensure that a user must be uniquely identified and authenticated before gaining access to the TOE management functions.

A.MANAGEMENT

- O.ADMIN provides the functionality that enables an authorised user to effectively manage the TOE and its security functions.

A.INSTALL

- O.INSTALL ensures that the TOE is delivered, installed, managed and operated in a manner that maintains security.

A.REMOTEMANAGEMENT

- O.ADMIN provides the functionality that enables an authorised user to effectively manage the TOE and its security functions.
- O.CONNECT and O.INSTALL ensure that the dedicated management port of the TOE is correctly connected and configured.

A.SNMP

- O.ADMIN provides the functionality that enables an authorised user to effectively manage the TOE and its security functions.
- O.CONNECT, O.INSTALL and O.PHYSICAL ensure that the dedicated management port of the TOE is correctly connected and configured.
- O.I&A provide the functionality for identifying and authenticating remote authorised users of the TOE.

A.PEER

- O.CONNECT, O.INSTALL, O.PHYSICAL and O.PERSONNEL ensure that the TOE is suitably connected to other protected ATM networks.

A.LOCATE

- O.PHYSICAL, O.INSTALL and O.CONNECT ensure that Cyphercell is installed in a secure environment.

A.CYPHERMANAGER

- O.PHYSICAL, O.INSTALL and O.CONNECT ensure that the CypherManager Management Station is installed in a secure environment.

A.ADMIN

- O.PERSONNEL ensures that only trusted and competent administrators are authorised to manage the TOE.

A.ATTACKERS

- All of the objectives are appropriate to protect the TOE against an attacker with a high level of expertise and resources and a low level of motivation.

T.CAPTURE

- O.FILTER allows for selected ATM cells to be encrypted or discarded according to a defined security policy.
- O.ENCRYPT allows for the encryption of ATM cell payloads.
- O.KEYMAN limits the exchange of keys to other authorised ATM encryptors.
- O.CERTIFICATE requires a valid X.509 certificate to be loaded into Cyphercell, which has been signed by CypherManager.
- O.CONNECT, O.INSTALL, O.PHYSICAL, and O.PERSONNEL support the four above objectives.

T.CONNECT

- O.ADMIN and O.ROLES provide essential support by ensuring secure administration of the TOE, in conjunction with the support provided by O.I&A, O.AUTHDATA, O.CONNECT, O.INSTALL, O.PHYSICAL, O.PERSONNEL.
- O.AUDIT and O.AUDITLOG monitor possible changes to the configuration of the TOE, allowing all authorised users to detect modifications.
- O.FILTER allows authorised users to explicitly allow connections, however, by default all connections, other than ATM management cells to the TOE, will be discarded.
- O.KEYMAN and O.CERTIFICATE ensure that encrypted connections cannot be made unless the originator and receiver holds a valid, signed, X.509 certificate.

T.ABUSE

- O.AUDIT and O.AUDITLOG monitor possible changes to the configuration of the TOE.
- O.ROLES prevents users from gaining access to, and performing operations on, the TOE's resources for which they are not explicitly authorised; i.e. enforces the concept of least privilege.
- O.AUTHDATA supports O.ROLES.
- O.PERSONNEL supports the above objectives by ensuring that only trusted and competent personnel operate the TOE.

T.ATTACK

- O.ADMIN and O.ROLES, supported by O.I&A, O.AUTHDATA, O.PERSONNEL protect against an attacker gaining access to and/or modifying the configuration information of the TOE.
- O.AUDIT supported by O.AUDITLOG monitor possible changes to the configuration of the TOE, allowing all authorised users to detect modifications.
- All of the above objectives are supported by O.CONNECT, O.PHYSICAL, and O.INSTALL.

T.IMPERSON

- O.ADMIN and O.ROLES, supported by O.AUTHDATA, O.I&A, O.PERSONNEL protect against an attacker gaining access to and/or modifying the configuration information of the TOE.
- O.AUDIT supported by O.AUDITLOG monitor possible changes to the configuration of the TOE, allowing all authorised users to detect modifications.
- O.KEYMAN supported by O.CERTIFICATE protect against an attacker establishing a connection to the TOE.
- All of the above objectives are supported by O.CONNECT, O.PHYSICAL, and O.INSTALL.

T.LINK

- O.FILTER allows authorised users to explicitly allow connections, however, by default, all connections to the TOE will be discarded.
- O.ENCRYPT allows for the encryption of ATM cell payloads.
- O.KEYMAN supported by O.CERTIFICATE restrict the number of possible communications paths to only other authorised TOEs.

T.OBSERVE

- O.ENCRYPT supported by O.KEYMAN and O.CERTIFICATE protects the confidentiality of information contained in the payload of the ATM cell.

T.PHYSICAL

- O.INSTALL, O.PHYSICAL and O.PERSONNEL ensure that the TOE is installed and operated in a secure environment by trusted users.

T.PRIVILEGE

- O.ROLES supported by O.PERSONNEL ensure that authorised trusted users have the minimum amount of access required to perform their duties.
- O.AUDIT supported by O.AUDITLOG monitor possible changes to the configuration of the TOE, allowing all authorised users to detect modifications.
- All the above objectives are supported by O.I&A and O.AUTHDATA.

P.CRYPTO

- O.ENCRYPT, O.KEYMAN and O.CERTIFICATE provide the confidentiality, authentication and key management services specified by this organisational security policy.

P.FILTER

- O.FILTER supported by O.ADMIN provide the traffic flow control specified in the organisational security policy.

P.ROLES

- O.ROLES supported by O.ADMIN provides for distinct user roles on the basis of least privilege as specified in the organisational security policy.

Given the arguments above in section 7.1.2 and the mapping’s shown in section 7.1.1, it has been demonstrated that the security objectives are suitable to counter all threats, and consider all assumptions and organisational security policies.

7.2 Security Requirements Rationale

7.2.1 Mapping of Security Functional Requirements (SFRs) to Objectives

Objectives	O.ADMIN	O.AUDIT	O.FILTER	O.ENCRYPT	O.I&A	O.ROLES	O.KEYMAN
Security Functional Requirements							
Identification & Authentication							
Identification of Users	🗳				🗳		
Authentication of Users	🗳				🗳		
Controls over creation, deletion or modification of user accounts						🗳	
Access Control							
Role based access control						🗳	
VCAT based access control			🗳				
Access Control Time			🗳				
Self Test							
Audit							
Generation of Audit Events		🗳					
Audit Trail Analysis & Review		🗳					
Audit Entry Timing		🗳					
Cryptographic Key Management							
Cryptographic Key Generation	🗳						🗳
Cryptographic Key Distribution							🗳
Cryptographic Key Destruction							🗳
Cryptographic Operations	🗳			🗳			
Authenticate X.509 Certificate Data for Certificate Load							
CKM Self Testing							🗳
Tamper Resistence							
Data Exchange							
Confidentiality of Management Data	🗳						
Confidentiality of Transmitted Information				🗳			
X.509 Certificate Management							
Generate Signed X.509 Certificates							
Protection of CM Private Key							
Authenticate X.509 Certificate Data							

Note:
Those SFRs common to both the CypherManager and Cyphercell components of the TOE have not been reproduced in the mappings.

Objectives Security Functional Requirements	O.AUDITLOG	O.AUTHDATA	O.CONNECT	O.INSTALL	O.PHYS	O.CERT	O.PERS
Identification & Authentication							
Identification of Users			🗳				
Authentication of Users			🗳				
Controls over creation, deletion or modification of user accounts							
Access Control							
Role based access control				🗳			
VCAT based access control			🗳				
Access Control Time			🗳				
Self Test				🗳			
Audit							
Generation of Audit Events				🗳			🗳
Audit Trail Analysis & Review	🗳						
Audit Entry Timing							
Cryptographic Key Management							
Cryptographic Key Generation						🗳	
Cryptographic Key Distribution							
Cryptographic Key Destruction							
Cryptographic Operations							
Authenticate X.509 Certificate Data for Certificate Load						🗳	
CKM Self Testing							
Tamper Resistance					🗳		
Data Exchange							
Confidentiality of Management Data			🗳				
Confidentiality of Transmitted Information							
X.509 Certificate Management							
Generate Signed X.509 Certificates						🗳	
Protection of CM Private Key						🗳	
Authenticate X.509 Certificate Data						🗳	

7.2.2 Informal Argument of Sufficiency

O.ADMIN

- *FDP_ITT.1* provides the capability for a protecting the confidentiality of management data such that an authorised user can remotely manage the TOE and its security functions in a manner required by O.ADMIN. *FIA_UID.2 and FIA_UAU.2* together ensure that only authorised users can access the functionality for managing the TOE as required by O.ADMIN.

O.AUDIT

- *FAU_GEN.1 and FAU_SAR.1* together provide the capability for generating and recording audit events in the manner required by O.AUDIT. *FPT_STM.1* ensures that a date and time stamp is recorded when these functions are invoked.

O.FILTER

- *FDP_ACC.1, FDP_ACF.1, FMT_MSA.1, FMT_MSA.2 and FMT_MSA.3* together provide the capability for authorised users to control traffic flow using ATM cell VPI/VCI information in a manner required by O.FILTER. *FPT_STM.1* provides the capability for controlling traffic flow on the basis of time of access.

O.ENCRYPT

- *FCS_COP.1, FDP_UCT.1 and FTP_ITC.1* provide the capability for encrypting information, and providing a trusted channel, to protect the confidentiality of information transferred across the ATM network required by O.ENCRYPT.

O.I&A

- *FIA_UID.2 and FIA_UAU.*2 provide the capability for identifying and authenticating all users in a manner required by O.I&A. *FMT_MTD.1* provides the capability for controlling creation, deletion and modification of user accounts on the basis of defined roles.

O.ROLES

- *FMT_SMR.1, FMT_MSA.1, FMT_MSA.2 and FMT_MSA.3* provide the capability for preventing access to TOE management facilities on the basis of defined roles required by O.ROLES.

O.KEYMAN

- *FCS_CKM.1, FCS_CKM.2 and FCS_CKM.4* provide the capability for generating, distributing and destroying cryptographic keys as required to provide means for exchanging keys with an authorised TOE as required by O.KEYMAN. *FPT_AMT.1* ensures the errors in the operation of these functions are detected.

O.AUDITLOG

- *FAU_SAR.1* provide the capability for viewing audit logs to support the effective use and management of the audit facilities in a manner required by O.AUDITLOG.

O.AUTHDATA

- *FTP_PHP.3* provides the capability for the TOE to protect against an attempt to gain physical access to localised user password information in a manner that supports O.AUTHDATA.

O.CONNECT

- *FIA_UID.2 and FIA_UAU.2* together provide the capability for identifying and authenticating users of the TOE by limiting connection to the management function to only authorised users of the TOE. *FDP_ACC.1, FDP_ACF.1, FMT_MSA.1, FMT_MSA.2 and FMT_MSA.3* together provide the capability to restrict connections to the public ATM network to only those entries listed in the VCAT. *FPT_STM.*1 provides the capability for allowing connections to the public ATM network, for any VPI/VCI in the VCAT, on the basis of time of access. *FDP_ITT.1*provides the capability for a trusted connection by a remote authorised user of the TOE for management of the TOE security functions.

O.INSTALL

- *FMT_SMR.1 FMT_MSA.1, FMT_MSA.2 and FMT_MSA.3* together provide the capability for allowing management of the TOE security functions on the basis of defined roles in a manner required for correct operation and management of the TOE. *FPT_AMT.1* provides the capability for the TOE to demonstrate correct operation by performing periodic self-tests and self-tests on startup.

O.PHYSICAL

- *FPT_PHP.3* provides the capability for the TOE to physically protect itself from compromise of key material via physical access to the TOE in a manner that supports O.PHYSICAL.
-

O.CERTIFICATE

- *FCS_CKM.1* provides the means for generating RSA Public/Private key pairs for both the Cyphercell and CypherManager. *FCS_COP.1* provides the means for signing completed X.509 certificates for the Cyphercell encryptor. *FDP_DAU.1* provides the means for producing a digest of the data for authentication purposes, when generating partial X.509 certificates in certificate load mode, and after sending completed and signed X.509 certificates from the CypherManager to the Cyphercell encryptor.

O.PERSONNEL

- *FAU_GEN.1 and FAU_SAR.1* provide the means for registering security relevant events that facilitate the detection of violations of security in the TOE in a manner that supports O.PERSONNEL. *FPT_STM.1* supports detection of security relevant events by associating each event with the date and time of the event.

Given the arguments above in section 7.2.2 and the mappings shown in section 7.2.1, it has been demonstrated that the security functional requirements are sufficient to enforce the security objectives for the TOE. However, the mappings shown in 7.2.1 are only complete for the TOE security objectives defined in section 4.1. The Environmental Security Objectives defined in section 4.2 may not necessarily be addressed, completely or partially, by the security functional requirements. For example, there are no security functional requirements in the TOE that will address the need for authorised users of the TOE to protect their own passwords from disclosure (O.AUTHDATA). The TOE environment addresses this objective, with the need for appropriately trained and trusted users, in conjunction with the procedures for storing password information external to the TOE.

As such, provision of an environment that satisfies the TOE environment security objectives is the responsibility of the owner of the Cyphercell ATM Encryptor. Determining whether the TOE environment satisfies the TOE environment security objectives is a matter for appropriate security authority assessing the system that incorporates the TOE.

7.2.3 Justification For Target Assurance Level

Common Criteria EAL4 has been chosen as the target level of assurance because the EAL4 level is considered appropriate for the protection of Australian Government information over public ATM networks. Further, the Cyphercell ATM Encryptor has been developed in Australia, which provides the evaluators with easy access to the developer, and associated low-level design information. Access to this information is necessary to provide the confidence that the TOE provides defence against the attacks as indicated in the Security Environment Section (Section 3) of this Security Target. Lastly, the developers expertise in engineering ATM technology will provide the evaluators with the necessary technical support to complete all the evaluation tasks for an EAL4 evaluation.

7.2.4 Strength of Function Claim

In general, an attacker would require access to domestic equipment, familiarity with ATM protocols, detailed knowledge of the encryption algorithms employed, and in the case of console port password attacks, physical access to the TOE. Based on the assumption A.ATTACKERS that attackers have a high level of expertise and resources, but a low level of motivation, the minimum strength of functions of the TOE is *basic*.

There are several security functions identified for the TOE where a “strength of function” claim is required. The majority of functions where the “strength of function” claim is required are cryptographic functions. DSD is the national authority for determining the appropriateness of any cryptographic functions. Therefore, no strength of function claim has been provided for cryptographic functions.

Users of the TOE must have passwords for generating authentication and privacy keys for SNMPv3 management. Given that these passwords are used to derive keys for the cryptographic components of the TOE, DSD will determine the appropriateness of the password-based key generation function of the TOE. Therefore, no strength of function claim has been provided for the password-based key generation function.

Users of the TOE may also access the Cyphercell component by console port logon. A user must present a User ID and an authentication password over the console port, which is then compared against the information contained in the user table. This I&A function is a probabilistic function, therefore a strength of function claim is required. Given that a user requires physical access to the Cyphercell component of the TOE to use the console, and the environmental objectives define constraints on the environment that limit such access, the minimum strength of the I&A function need only be *basic*.

7.2.5 SFR Dependencies Analysis

The table below shows those components that are dependent on other SFRs of the TOE.

Component:	Depends On:	Which Is:
FIA_UAU.2	FIA_UID1.	Not included. FIA_UID.2 used
FMT_MTD.1	FMT_SMR.1	Included
FMT_SMR.1	FMT_UID.1	Not included. FIA_UID.2 used.
FMT_MSA.1	FDP_ACC.1 FMT_SMR.1	Included Included
FMT_MSA.2	ADV_SPM.1 FDP_ACC.1 FMT_MSA.1 FMT_SMR.1	Refer to TOE Informal Security Policy Model Included Included Included
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Included Included
FDP_ACC.1	FDP_ACF.1	Included
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3 FPT_STM.1	Included Included Included. Required for time based VCAT.
FAU_GEN.1	FPT_STM.1	Included
FAU_SAR.1	FAU_GEN.1	Included
FCS_CKM.1	FCS_COP.1 FCS_CKM.4 FCS_MSA.2	Included Included Included
FCS_CKM.2	FCS_CKM.1 FDP_ITC.1 FCS_CKM.4 FMT_MSA.2	Included Included Included Included
FCS_CKM.4	FDP_ITC.1 FCS_CKM.1 FMT_MSA.2	Included Included Included
FCS_COP.1	FDP_ITC.1 FCS_CKM.1 FCS_CKM.4 FMT_MSA.2	Included Included Included Included
FDP_UCT.1	FTP_ITC.1 FDP_ACC.1	Included Included
FPT_ITT.1	FCS_COP.1	Included. Required for encryption of transferred data
FDP_DAU.1	FCS_COP.1	Included. Required for MD5

7.2.6 Demonstration of Mutual Support

The analysis to demonstrate mutual support considers attacks in four main areas. Statements on how the TOE security functions mutually support each other in preventing these attacks are provided below:

Tamper attacks are prevented by:

- *Security functions that restrict the modification of attributes or configuration data to authorised administrators and supervisors only (e.g. those based on FMT_MSA.1).*
- *Security functions that prevent the unauthorised modification of other data, the integrity of which is critical to a security function (i.e. those based on FMT_MTD.1).*
- *Security functions that protect the confidentiality of management information from the remote management host (CypherManager) to the Cyphercell (i.e. FPT_ITT.1).*
- *Security functions that protect against 'man-in-the-middle' attacks by authenticating data generated during X.509 certificate loading of the TOE (ie. FDP_DAU.1].*

Bypassing attacks are prevented by:

- *Security functions that require user identification and user authentication prior to allowing the user to perform actions on the security attributes of the TOE (based on FIA_UAU.2, FIA_UID.2). These are stronger properties than those based in FIA_UAU.1 and FIA_UID.1.*
- *Security functions that allow for handling of ATM traffic on the basis of VPI/VCI header information. (i.e. FDP_ACC.1).*
- *FPT_STM.1 that provides reliable time stamping for handling of ATM traffic.*

Failure of Detection of Misconfiguration is prevented by:

- *Security functions that capture security relevant events (e.g. unsuccessful user identification and authentication) (based on FAU_GEN.1)*
- *Security functions that provide security relevant audit data in a readable form to allow for detection of misconfigurations (based on FAU_SAR.1)*
- *FPT_STM.1 that provides reliable time stamping for each security relevant event.*
- *Abstract machine testing that allows for the determination of correct/incorrect operation of the abstract machine that underlies all other security functions (FPT_AMT.1).*
- *FPT_PHP.3 which resists an attempt to gain physical access to the key material and password data, and takes automatic action.*

Breach of Transmitted Information Confidentiality is prevented by:

- *Security functions that provide a trusted communications channel between the TOE and a remote instance of the TOE (FTP_ITC.1).*
- *Security functions that provide for key generation, key distribution and key destruction (FCS_CKM.1, FCS_CKM.2 and FCS_CKM.4).*
- *Security functions that allow only secure values are accepted for secure attributes (FMT_MSA.1).*

The tables provided in section 7.2.5 show those security functions that are dependent upon other security functions of the TOE. The informal analysis provided above, shows how those dependent security functions are mutually supportive in satisfying the security functional requirements of the TOE.

7.3 TOE Summary Specification Rationale

7.3.1 Table of SFRs versus TOE Security Functions

SFR TOE Security Function	Identification of Users	Authentication of Users	Controls over creation, deletion or modification of user accounts	Role-based access control	VCAT based access control	Generation of Audit Events	Audit Trail Analysis and Review
FIA_UID.2.1	✓						
FIA_UAU.2.1		✓					
FMT_SMR.1.1				✓			
FMT_SMR.1.2				✓			
FDP_ACC.1.1.A					✓		
FDP_ACC.1.1.B				✓			
FDP_ACC.1.1.C				✓			
FDP_ACF.1.1.A					✓		
FDP_ACF.1.1.B				✓			
FDP_ACF.1.1.C				✓			
FDP_ACF.1.2.A					✓		
FDP_ACF.1.2.B				✓			
FDP_ACF.1.2.C				✓			
FDP_ACF.1.3.A					✓		
FDP_ACF.1.3.B				✓			
FDP_ACF.1.3.C				✓			
FDP_ACF.1.4.A					✓		
FDP_ACF.1.4.B				✓			
FDP_ACF.1.4.C				✓			
FAU_GEN.1.1						✓	
FAU_GEN.1.2						✓	
FAU_SAR.1.1							✓
FAU_SAR.1.2							✓
FCS_CKM.1.1.A							
FCS_CKM.1.1.B							
FCS_CKM.1.1.C							
FCS_CKM.2.1							
FCS_CKM.4.1							
FCS_COP.1.1.A							
FCS_COP.1.1.B							
FCS_COP.1.1.C							
FCS_COP.1.1.D							
FCS_COP.1.1.E							
FDP_UCT.1.1							
FTP_ITC.1.1							
FTP_ITC.1.2							
FTP_ITC.1.3							
FPT_STM.1.1					✓	✓	
FPT_AMT.1.1							
FPT_PHP.3.1.A							
FPT_PHP.3.1.B							
FMT_MSA.1.1.A					✓		
FMT_MSA.1.1.B				✓			
FMT_MSA.1.1.C				✓			
FMT_MSA.2.1				✓	✓		
FMT_MSA.3.1.A					✓		
FMT_MSA.3.1.B				✓			
FMT_MSA.3.1.C				✓			
FMT_MSA.3.2				✓	✓		
FMT_MTD.1.1			✓				
FDP_DAU.1.1							

SFR TOE Security Function	Identification of Users	Authentication of Users	Controls over creation, deletion or modification of user accounts	Role-based access control	VCAT based access control	Generation of Audit Events	Audit Trail Analysis and Review
FDP_DAU.1.2							
FPT_ITT.1.1							

SFR TOE Security Function	Cryptographic Key Generation	Cryptographic Key Distribution	Cryptographic Key Destruction	Cryptographic Operations	Confidentiality of Management Data	Confidentiality of Transmitted Information
FIA_UID.2.1						
FIA_UAU.2.1						
FMT_SMR.1.1						
FMT_SMR.1.2						
FDP_ACC.1.1.A						
FDP_ACC.1.1.B						
FDP_ACC.1.1.C						
FDP_ACF.1.1.A						
FDP_ACF.1.1.B						
FDP_ACF.1.1.C						
FDP_ACF.1.2.A						
FDP_ACF.1.2.B						
FDP_ACF.1.3.C						
FDP_ACF.1.3.A						
FDP_ACF.1.3.B						
FDP_ACF.1.3.C						
FDP_ACF.1.4.A						
FDP_ACF.1.4.B						
FDP_ACF.1.4.C						
FAU_GEN.1.1						
FAU_GEN.1.2						
FAU_SAR.1.1						
FAU_SAR.1.2						
FCS_CKM.1.1.A	🗳					
FCS_CKM.1.1.B	🗳					
FCS_CKM.1.1.C	🗳					
FCS_CKM.2.1		🗳				
FCS_CKM.4.1			🗳			
FCS_COP.1.1.A				🗳		
FCS_COP.1.1.B				🗳		
FCS_COP.1.1.C				🗳		
FCS_COP.1.1.D				🗳		
FCS_COP.1.1.E				🗳		
FDP_UCT.1.1						🗳
FTP_ITC.1.1						🗳
FTP_ITC.1.2						🗳
FTP_ITC.1.3						🗳
FPT_STM.1.1				🗳		
FPT_AMT.1.1				🗳		
FPT_PHP.3.1.A				🗳		
FPT_PHP.3.1.B					🗳	
FMT_MSA.1.1.A						
FMT_MSA.1.1.B						
FMT_MSA.1.1.C						
FMT_MSA.2.1						
FMT_MSA.3.1.A						
FMT_MSA.3.1.B						
FMT_MSA.3.1.C						

SFR TOE Security Function	Cryptographic Key Generation	Cryptographic Key Distribution	Cryptographic Key Destruction	Cryptographic Operations	Confidentiality of Management Data	Confidentiality of Transmitted Information
FMT_MSA.3.2						
FMT_MTD.1.1						
FDP_DAU.1.1						
FDP_DAU.1.2						
FPT_ITT.1.1					✓	

SFR TOE Security Function	Generate Signed X.509 Certificates	Authenticate X.509 Certificates & Requests
FIA_UID.2.1		
FIA_UAU.2.1		
FMT_SMR.1.1		
FMT_SMR.1.2		
FDP_ACC.1.1.A		
FDP_ACC.1.1.B		
FDP_ACC.1.1.C		
FDP_ACF.1.1.A		
FDP_ACF.1.1.B		
FDP_ACF.1.1.C		
FDP_ACF.1.2.A		
FDP_ACF.1.2.B		
FDP_ACF.1.3.C		
FDP_ACF.1.3.A		
FDP_ACF.1.3.B		
FDP_ACF.1.3.C		
FDP_ACF.1.4.A		
FDP_ACF.1.4.B		
FDP_ACF.1.4.C		
FAU_GEN.1.1		
FAU_GEN.1.2		
FAU_SAR.1.1		
FAU_SAR.1.2		
FCS_CKM.1.1.A		
FCS_CKM.1.1.B		
FCS_CKM.1.1.C	✓	
FCS_CKM.2.1		
FCS_CKM.4.1		
FCS_COP.1.1.A		
FCS_COP.1.1.B	✓	
FCS_COP.1.1.C		✓
FCS_COP.1.1.D	✓	
FCS_COP.1.1.E		
FDP_UCT.1.1		
FTP_ITC.1.1		
FTP_ITC.1.2		
FTP_ITC.1.3		
FPT_STM.1.1		
FPT_AMT.1.1		
FPT_PHP.3.1.A		
FPT_PHP.3.1.B		
FMT_MSA.1.1.A		
FMT_MSA.1.1.B		
FMT_MSA.1.1.C		
FMT_MSA.2.1		
FMT_MSA.3.1.A		
FMT_MSA.3.1.B		
FMT_MSA.3.1.C		
FMT_MSA.3.2		

SFR TOE Security Function	Generate Signed X.509 Certificates	Authenticate X.509 Certificates & Requests
FMT_MTD.1.1		
FDP_DAU.1.1		✓
FDP_DAU.1.2		✓
FPT_ITT.1.1		

7.3.2 Demonstration of Suitability

From the tables mapping TOE Security Functions (TSFs) to the Security Functional Requirements (SFRs), there is a clear one-to-one mapping for the following TSFs and SFRs:

Identification of Users and FIA_UID.2.1
Authentication of Users and FIA_UAU.2.1
Controls over creation, deletion or modification of user accounts and FMT_MTD.1.1
Cryptographic Key Distribution and FCS_CKM.2.1
Cryptographic Key Destruction and FCS_CKM.4.1

Given that the TOE Security functions and the SFRs were derived from part 2 of the Common Criteria, the mapping is self evident, and therefore these TSFs are suitable to meet their Security Functional Requirements.

The analysis of the remaining SFRs that are satisfied by more than one TSF is provided below:

Role-Based Access Control

- *FDP_ACC.1.1B* provides the functionality to enforce the *Remote Management Access Control SFP* SNMPv3 packets received on the Ethernet management port.
- *FDP_ACC.1.1.C* to enforce the *Local Management Access Control SFP* on the console management port.
- *FDP_ACF.1.1.B, FDP_ACF.1.2.B, FDP_ACF.1.3.B, FDP_ACF.1.4.B* together provide the necessary functionality for enforcing the *Remote Management Access Control* based on user ID, User password and user role.
- *FDP_ACF.1.1.C, FDP_ACF.1.2.C, FDP_ACF.1.3.C, FDP_ACF.1.4.C* together provide the necessary functionality for enforcing the *Local Management Access Control* based on user ID, User password and user role.
- *FMT_SMR.1.1* and *FMT_SMR.1.2* together provide the functionality to maintain user roles and associate roles with users.
- *FMT_MSA.1.1.B* restricts the ability of remote users to modify the security attributes of the TOE based on the defined roles.
- *FMT_MSA.1.1.C* restricts the ability of local users to modify the security attributes of the TOE based on the defined roles.
- *FMT_MSA.2.1* ensures that, if modification of security attributes is permitted by a user role, then only secure values are accepted for those security attributes.
- *FMT_MSA.3.1.B, FMT_MSA.3.1.C* and *FMT_MSA.3.2* ensure that, by default, restrictive values are used to enforce the *Remote Management Access Control SFP* and that overriding initial default values is restricted on the basis of the defined user roles.

VCAT Based Access Control

- *FDP_ACC.1.1* ensures that the *cell control SFP* is enforced for all ATM cells received on the interfaces of the TOE.
- *FDP_ACF.1.1*, *FDP_ACF.1.2*, *FDP_ACF.1.3* and *FDP_ACF.1.4* together provide the necessary functionality for enforcing the *cell control SFP* and determining the actions on received ATM cells on the basis of their *VPI/VCI* header information.
- *FMT_STM.1.1* provides reliable time stamping for determining if an operation on an ATM Cell is allowed on the basis of time of access.
- *FMT_MSA.1.1.A* ensures that the *cell control SFP* is enforced to restrict the ability to encrypt, bypass or discard ATM cells received at the TOE interface to those cells whose VPI/VCI is listed in the VCAT.
- *FMT_MSA.2.1* ensures that only secure values are accepted into the VCAT table.

- *FMT_MSA.3.1.A* and *FMT_MSA.3.2* together ensure that, by default, restrictive values are used to enforce the *cell control SFP* and that overriding initial default values is restricted on the basis of the defined user roles.

Generation of Audit Events

- *FAU_GEN.1.1* and *FAU_GEN.1.2* together ensure that audit records are generated and contain relevant information about the security relevant event.
- *FMT_STM.1.1* ensures that reliable time stamps are generated that can be associated with each audit event.

Audit Trail Analysis and Review

- *FAU_SAR.1.1* and *FAU_SAR.1.2* together ensure that authorised users can read audit information from the audit records. *FAU_SAR.1.1* provides the capability for reviewing audit records, whereas, *FAU_SAR.1.2* presents audit information in a manner suitable for interpretation.

Cryptographic Key Generation

- *FCS_CKM.1.1.A, FCS_CKM.1.1.B and FCS_CKM.1.1.C* specify the algorithms used for generating all the keys necessary for the operation of the TOE.

Cryptographic Operations

- *FCS_COP.1.1.A, FCS_COP.1.1.B, FCS_COP.1.1.C, FCS_COP.1.1.D and FCS_COP.1.1.E,* define the cryptographic operations of the TOE.
- *FCS_COP.1.1.A* specifies the cryptographic operation performed on the payload of transmitted ATM cells.
- *FCS_COP.1.1.B* specifies the cryptographic operation for transferring initial master and session keys between instances of the TOE that are used for encrypting ATM cell payloads and for transferring the administrator passwords during X.509 certificate loading.
- *FCS_COP.1.1.C* specifies the cryptographic operation for transferring session keys between instances of the TOE that are used for encrypting ATM cell payloads and for calculating a secure hash of data for X.509 certificate loading.
- *FCS_COP.1.1.D* specifies the cryptographic operation for signing X.509 certificates.
- *FCS_COP.1.1.E* specifies the cryptographic operation performed on the data in the SNMP command.
- *FMT_STM.1.1* ensures that reliable time stamps are generated that can be used to control the updating of session keys for any *VPI/VCI* in the VCAT.
- *FPT_PHP.3.1.A* ensures that the cryptographic operations are protected from compromise of the key material, that could be used to gain access to the transmitted information.
- *FPT_AMT.1.1* ensures that cryptographic operations are regularly checked to demonstrate correct operation.

Confidentiality of Management Data

- *FPT_ITT.1.1* ensures that all TSF (management) data passed between CypherManager and Cyphercell using SNMPv3 is appropriately protected.
- *FPT_PHP.3.1.B* ensures that the TOE protected from compromise of password data that could be used to gain remote access to the TOE, for the purposes of gaining access to the management functions of the TOE.

Confidentiality of Transmitted Information

- *FDP_UCT.1.1.B, FTP_ITC.1.1, FTP_ITC.1.2* and *FTP_ITC.1.3* together provide a trusted communications channel that is logically distinct from other communications channels with remote instances of the TOE, in a manner that protects the transmitted information from unauthorised disclosure.

Generate Signed X.509 Certificates

- *FCS_CKM.1.1C, FCS_COP.1.1.B and FCS_COP.1.1.D* together provide the necessary cryptographic functionality to sign X.509 certificates.

Authenticate X.509 Certificate & Requests

- *FDP_DAU.1.1 and FDP_DAU.1.2* together provide the necessary functionality for administrators to verify the authenticity of X.509 certificate data when generating loading X.509 certificates into the TOE.
- *FCS_COP.1.1.C* provides the cryptographic functionality to calculate a hash of the data for verification.

From the mappings provided in section 7.3.1 it can be clearly seen that all TSFs map to at least one SFR and also that all SFRs map to at least one TSF. Given the arguments above and the complete mappings shown in section 7.3.1, and the fact that all TSFs and SFRs were derived from the Common Criteria Part 2: Security Functional Requirements, it can be concluded that the TOE security functions are suitable to meet the security functional requirements for the TOE.

7.3.3 Demonstration of Mutual Support

It is not necessary to repeat an analysis of TOE Security Function binding at this level given that:

a. All functions at this level were derived from the Security Functional Requirements identified in section 5.0 of the Security Target; and

b. In section 7.2 all security functions were shown to bind together to provide a mutually supportive and effective whole.

Therefore, it is possible to conclude that all TOE Security Functions identified at this level bind together to provide a mutually supportive and effective whole.

7.3.4 Assurance Requirements Rationale

The requirements for EAL4 level of assurance were justified in section 7.2.3. of this Security Target.